(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4281252号
(P4281252)

(45)発行日　平成21年6月17日(2009.6.17)　(24)登録日　平成21年3月27日(2009.3.27)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	560C
G09C 1/00	(2006.01)	G06F	12/14	540P
G11B 20/10	(2006.01)	G09C	1/00	640D
G11B 20/12	(2006.01)	G11B	20/10	H
H04L 9/08	(2006.01)	G11B	20/12	

請求項の数 13　(全 49 頁)　最終頁に続く

(21)出願番号　特願2001-7238(P2001-7238)
(22)出願日　平成13年1月16日(2001.1.16)
(65)公開番号　特開2002-215465(P2002-215465A)
(43)公開日　平成14年8月2日(2002.8.2)
審査請求日　平成17年5月25日(2005.5.25)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100086531
弁理士　澤田　俊夫
(72)発明者　瀧　隆太
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　浅野　智之
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム記憶媒体

(57)【特許請求の範囲】

【請求項１】

記録媒体に対するデータ記録処理を実行する情報記録装置において、

記録媒体に格納するコンテンツの暗号化処理を実行し暗号化コンテンツを生成するとともに、コンテンツの利用制限情報を含むコンテンツの権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）を生成する暗号処理手段と、

記録媒体に対するデータ記録処理を実行する記録部を有し、

前記記録部は、前記記録媒体の物理的保護領域に対する前記改竄チェック値（ＩＣＶ）の記録処理に適用し、前記暗号化コンテンツの記録処理には適用することのない秘密情報記録専用回路を有し、

前記暗号処理手段は、

階層ツリー構造におけるリーフを構成する選択された情報記録装置においてのみ復号可能な有効化キーブロック（ＥＫＢ）の復号処理によって取得されるＥＫＢキーを適用して、前記権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）の生成に適用するＩＣＶキーを生成し、さらに、前記ＥＫＢキーを適用してコンテンツ暗号化に適用するコンテンツキーの暗号化を実行して暗号化コンテンツキーを生成し、

前記記録部は、

前記暗号化コンテンツと、前記有効化キーブロック（ＥＫＢ）と、前記暗号化コンテンツキー、および前記権利管理（ＤＲＭ）データを通常のデータ記録再生処理の適用領域であるユーザ領域に記録し、

前記改竄チェック値（ＩＣＶ）を、専用回路によってのみ記録再生が可能な保護領域に記録する構成であることを特徴とする情報記録装置。

【請求項２】

前記権利管理（ＤＲＭ）データは、

コンテンツの利用に関する情報、コンテンツの暗号化キーとしてのコンテンツキーを暗号化した暗号化コンテンツキー、およびコンテンツ識別子（ＩＤ）を含むものであることを特徴とする請求項１に記載の情報記録装置。

【請求項３】

前記秘密情報記録専用回路は、前記コンテンツの記録方式に適用する信号処理と異なる信号処理を適用して前記改竄チェック値（ＩＣＶ）の前記記録媒体の物理的保護領域に対する記録処理を実行する構成を有することを特徴とする請求項１に記載の情報記録装置。

【請求項４】

前記秘密情報記録専用回路は、前記コンテンツの記録方式に適用する信号処理と異なる信号処理を適用して前記改竄チェック値（ＩＣＶ）の前記記録媒体の物理的保護領域に対する記録処理を実行する構成を有するとともに、

前記秘密情報記録専用回路は、前記改竄チェック値（ＩＣＶ）を含む秘密情報を、対応コンテンツの記録媒体における記録領域に重畳する領域に記録する処理を実行する構成を有することを特徴とする請求項１に記載の情報記録装置。

【請求項５】

前記暗号処理手段は、

コンテンツの記録媒体に対する記録処理において、該コンテンツに対応する権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）が付加されている場合は、該ＩＣＶの検証処理を実行し、権利管理（ＤＲＭ）データの改竄のないことが検証されたことを条件としてコンテンツの記録媒体に対する記録処理に伴う処理を実行する構成を有することを特徴とする請求項１に記載の情報記録装置。

【請求項６】

前記暗号処理手段は、

コンテンツの記録媒体に対する記録処理において、該コンテンツが他の装置からの送信コンテンツである場合、他装置との間における相互認証の成立を条件としてコンテンツの記録媒体に対する記録処理に伴う処理を実行する構成を有することを特徴とする請求項１に記載の情報記録装置。

【請求項７】

前記情報記録装置は、

コンテンツの記録媒体に対する記録処理において、前記権利管理（ＤＲＭ）データの更新を実行した場合に、前記暗号処理手段において、該更新された権利管理（ＤＲＭ）データに基づく改竄チェック値（ＩＣＶ）を生成し、記録媒体に更新された権利管理（ＤＲＭ）データに基づく更新改竄チェック値（ＩＣＶ）を記録する構成であることを特徴とする請求項１に記載の情報記録装置。

【請求項８】

記録媒体からのデータ再生処理を実行する情報再生装置において、

記録媒体に格納されたコンテンツの復号処理を実行するとともに、コンテンツの利用制限情報を含むコンテンツの権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）の検証を実行する暗号処理手段と、

前記記録媒体の物理的保護領域からの前記改竄チェック値（ＩＣＶ）の再生処理に適用し、前記暗号化コンテンツの再生処理には適用することのない秘密情報再生専用回路を有し、

前記暗号処理手段は、

階層ツリー構造におけるリーフを構成する選択された情報再生装置においてのみ復号可能な有効化キーブロック（ＥＫＢ）の復号処理によって取得されるＥＫＢキーを適用して、前記権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）の生成に適用するＩＣＶキ

ーを生成し、生成したＩＣＶキーを適用して前記権利管理（ＤＲＭ）データの改竄チェック処理を実行し、改竄無しの確認を条件として、前記ＥＫＢキーを適用してコンテンツ復号に適用する暗号化コンテンツキーの復号を実行してコンテンツキーを生成し、生成したコンテンツキーにより、暗号化コンテンツの復号処理を行うことを特徴とする情報再生装置。

【請求項９】

前記権利管理（ＤＲＭ）データは、

コンテンツの利用に関する情報、コンテンツの暗号化キーとしてのコンテンツキーを暗号化した暗号化コンテンツキー、およびコンテンツ識別子（ＩＤ）を含むものであることを特徴とする請求項８に記載の情報再生装置。

【請求項１０】

前記秘密情報再生専用回路は、前記コンテンツの再生方式に適用する信号処理と異なる信号処理を適用して前記改竄チェック値（ＩＣＶ）の前記記録媒体の物理的保護領域からの再生処理を実行する構成を有することを特徴とする請求項８に記載の情報再生装置。

【請求項１１】

前記秘密情報再生専用回路は、前記コンテンツの再生方式に適用する信号処理と異なる信号処理を適用して前記改竄チェック値（ＩＣＶ）の前記記録媒体の物理的保護領域からの再生処理を実行する構成を有するとともに、

前記秘密情報再生専用回路は、前記改竄チェック値（ＩＣＶ）を含む秘密情報を、対応コンテンツの記録媒体における記録領域に重畳する領域から再生する処理を実行する構成を有することを特徴とする請求項８に記載の情報再生装置。

【請求項１２】

情報記録装置において、記録媒体に対するデータ記録処理を実行する情報記録方法であり、

暗号処理手段が、記録媒体に格納するコンテンツの暗号化処理を実行し暗号化コンテンツを生成するとともに、コンテンツの利用制限情報を含むコンテンツの権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）を生成する暗号処理ステップと、

記録部が、記録媒体に対するデータ記録処理を実行する記録ステップを有し、

前記暗号処理ステップは、

階層ツリー構造におけるリーフを構成する選択された情報記録装置においてのみ復号可能な有効化キーブロック（ＥＫＢ）の復号処理によって取得されるＥＫＢキーを適用して、前記権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）の生成に適用するＩＣＶキーを生成し、さらに、前記ＥＫＢキーを適用してコンテンツ暗号化に適用するコンテンツキーの暗号化を実行して暗号化コンテンツキーを生成するステップであり、

前記記録ステップは、

前記暗号化コンテンツと、前記有効化キーブロック（ＥＫＢ）と、前記暗号化コンテンツキー、および前記権利管理（ＤＲＭ）データを通常のデータ記録再生処理の適用領域であるユーザ領域に記録し、

前記改竄チェック値（ＩＣＶ）を、専用回路によってのみ記録再生が可能な保護領域に記録するステップであることを特徴とする情報記録方法。

【請求項１３】

情報再生装置において、記録媒体からのデータ再生処理を実行する情報再生方法であり、

暗号処理手段が、記録媒体に格納されたコンテンツの復号処理を実行するとともに、コンテンツの利用制限情報を含むコンテンツの権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）の検証を実行する暗号処理ステップと、

再生手段が、記録媒体からのデータ再生処理を実行する再生ステップを有し、

前記暗号処理ステップは、

階層ツリー構造におけるリーフを構成する選択された情報再生装置においてのみ復号可能な有効化キーブロック（ＥＫＢ）の復号処理によって取得されるＥＫＢキーを適用して

、前記権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）の生成に適用するＩＣＶキーを生成し、生成したＩＣＶキーを適用して前記権利管理（ＤＲＭ）データの改竄チェック処理を実行し、改竄無しの確認を条件として、前記ＥＫＢキーを適用してコンテンツ復号に適用する暗号化コンテンツキーの復号を実行してコンテンツキーを生成し、生成したコンテンツキーにより、暗号化コンテンツの復号処理を行うステップを含むことを特徴とする情報再生方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム記憶媒体に関し、特に、利用制限の付加されたデジタルコンテンツデータの利用処理を適切に実行可能とした装置および方法に関する。特に、木構造の階層的鍵配信方式を用いて有効化キーブロック（ＥＫＢ：Enabling Key Block）キーを提供し、ＥＫＢキーを用いてコンテンツに関する権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）を生成してコンテンツの正当な利用を可能とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム記憶媒体に関する。

【０００２】

【従来の技術】

現在、ＤＡＴ、ＣＤ、ＤＶＤなどデジタルデータの記録可能な媒体が流通し、音楽データ、画像データなどの様々なコンテンツがデジタルデータとしてこれらの媒体に記録され広く流通している。

【０００３】

このようなデジタルデータは、アナログデータと異なり、記録媒体間デのデータコピーにおけるデータの劣化がなく、コピーを無制限に許容すると、コンテンツの著作者、あるいはその他コンテンツに関する権利者の権利が阻害されるおそれがある。このようなデジタルデータの権利保護のため、著作権保護技術としてＳＣＭＳ（Serial Copy Management System）がある。

【０００４】

ＳＣＭＳ（Serial Copy Management System）は、デジタルデータのコピー制限システムであり、1世代（1-Generation）のみのコピーのみを許容し、２世代以降のデジタルコピーを禁止するものである。具体的には、デジタルデータとして記録された媒体（メディア）にコピーを１回のみ許容することを示すコードを記録し、このコードに基づいてコピー制限を行なっている。

【０００５】

しかし、このＳＣＭＳによる１世代コピーコントロールは、コピーを１回のみ許容することを示す媒体上の記録コード、すなわちビットの状態によりコピー可・不可が判断される構成であり、このビットを任意に操作できるデバイスを用いればコードの書き替えが可能となり、オリジナルデータと同じコピーを多数作ることが出来てしまう。このため、特に法律の制約を受けないＰＣを用いたＣＤ等のデジタルデータ記録媒体のコピーは事実上野放しになっている。

【０００６】

一方、著作権の保護を目的とした映像、音楽などのコンテンツを記録、再生するシステムには、コンテンツを暗号化してユーザに提供し、正規なユーザにのみ暗号を解く鍵を提供するシステムが提案されている。

【０００７】

例えばインターネット、あるいはＣＤ、ＤＶＤなどのメディアを介して暗号化された音声データ、画像データ、ゲームプログラム等の各種コンテンツをユーザに配布し、正規ユーザであると確認された者に対してのみ、配布された暗号化コンテンツを復号する手段、すなわち復号鍵を付与するシステム構成である。

【０００８】
暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。
【０００９】
暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類あるが、その１つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にＤＥＳ（データ暗号標準：Deta encryption standard）がある。
【００１０】
上述の暗号化処理、復号化に用いられる暗号化鍵、復号化鍵は、例えばあるパスワード等に基づいてハッシュ関数等の一方向性関数を適用して得ることができる。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めることは実質上不可能となる。
【００１１】
また、暗号化するときに使用する暗号化鍵による処理と、復号するときに使用する復号化鍵の処理とを異なるアルゴリズムとした方式がいわゆる公開鍵暗号化方式と呼ばれる方式である。公開鍵暗号化方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が発行した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号処理が可能となる。秘密鍵は、公開鍵を発行した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号化方式の代表的なものにはＲＳＡ（Rivest-Shamir-Adleman）暗号がある。このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。
【００１２】
このようなシステムではコピー制御情報として、例えば２ビットのＥＭＩ(Encryption Mode Indicator)が規定されている。ＥＭＩが００Ｂ（Ｂは、その前の値が２進数であることを表す）である場合は、コンテンツがコピーフリーのもの(Copy-freely)であることを表し、ＥＭＩが０１Ｂである場合には、コンテンツが、それ以上のコピーをすることができないもの(No-more-copies)であることを表す。さらに、ＥＭＩが１０Ｂである場合は、コンテンツが、１度だけコピーして良いもの(Copy-one-generation)であることを表し、ＥＭＩが１１Ｂである場合には、コンテンツが、コピーが禁止されているもの(Copy-never)であることを表す。
【００１３】
ＥＭＩが、Copy-freelyやCopy-one-generationであるときには、コンテンツはコピー可能であると判定される。また、ＥＭＩが、No-more-copiesやCopy-neverであるときには、コンテンツはコピー可能でないと判定される。このようなコピールール情報の管理が適切に実行されれば、著作権の保護が実現される。
【００１４】
しかしながら、このような暗号化を用いたコンテンツの提供システムにおいても、例えばＣＤ、ＤＶＤなどの媒体に記録されたコピールールを示す情報が不正なユーザによって書き換えられてしまうと、本来のコピールールを無視したコピーが実行可能となってしまうという問題がある。
【００１５】
【発明が解決しようとする課題】

本発明は、上記のようなデータコピー、またはデータ再生の実行における不正なコンテンツの利用を排除し、正当なユーザにおける正当なコンテンツ利用のみを許容することを可能とする情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム記憶媒体を提供することを目的とする。

【００１６】

【課題を解決するための手段】

本発明の第１の側面は、

記録媒体に対するデータ記録処理を実行する情報記録装置において、

記録媒体に格納するコンテンツの暗号化処理を実行し暗号化コンテンツを生成するとともに、コンテンツの利用制限情報を含むコンテンツの権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）を生成する暗号処理手段と、

記録媒体に対するデータ記録処理を実行する記録部を有し、

前記記録部は、前記記録媒体の物理的保護領域に対する前記改竄チェック値（ＩＣＶ）の記録処理に適用し、前記暗号化コンテンツの記録処理には適用することのない秘密情報記録専用回路を有し、

前記暗号処理手段は、

階層ツリー構造におけるリーフを構成する選択された情報記録装置においてのみ復号可能な有効化キーブロック（ＥＫＢ）の復号処理によって取得されるＥＫＢキーを適用して、前記権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）の生成に適用するＩＣＶキーを生成し、さらに、前記ＥＫＢキーを適用してコンテンツ暗号化に適用するコンテンツキーの暗号化を実行して暗号化コンテンツキーを生成し、

前記記録部は、

前記暗号化コンテンツと、前記有効化キーブロック（ＥＫＢ）と、前記暗号化コンテンツキー、および前記権利管理（ＤＲＭ）データを通常のデータ記録再生処理の適用領域であるユーザ領域に記録し、

前記改竄チェック値（ＩＣＶ）を、専用回路によってのみ記録再生が可能な保護領域に記録する構成であることを特徴とする情報記録装置にある。

【００１７】

さらに、本発明の情報記録装置の一実施態様において、前記権利管理（ＤＲＭ）データは、コンテンツの利用に関する情報、コンテンツの暗号化キーとしてのコンテンツキーを暗号化した暗号化コンテンツキー、およびコンテンツ識別子（ＩＤ）を含むものであることを特徴とする。

【００１８】

さらに、本発明の情報記録装置の一実施態様において、前記秘密情報記録専用回路は、前記コンテンツの記録方式に適用する信号処理と異なる信号処理を適用して前記改竄チェック値（ＩＣＶ）の前記記録媒体の物理的保護領域に対する記録処理を実行する構成を有することを特徴とする。

【００１９】

さらに、本発明の情報記録装置の一実施態様において、前記秘密情報記録専用回路は、前記コンテンツの記録方式に適用する信号処理と異なる信号処理を適用して前記改竄チェック値（ＩＣＶ）の前記記録媒体の物理的保護領域に対する記録処理を実行する構成を有するとともに、前記秘密情報記録専用回路は、前記改竄チェック値（ＩＣＶ）を含む秘密情報を、対応コンテンツの記録媒体における記録領域に重畳する領域に記録する処理を実行する構成を有することを特徴とする。

【００２６】

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、コンテンツの記録媒体に対する記録処理において、該コンテンツに対応する権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）が付加されている場合は、該ＩＣＶの検証処理を実行し、権利管理（ＤＲＭ）データの改竄のないことが検証されたことを条件としてコンテンツの記録媒体に対する記録処理に伴う処理を実行する構成を有することを特徴とする。

【００２７】
さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、コンテンツの記録媒体に対する記録処理において、該コンテンツが他の装置からの送信コンテンツである場合、他装置との間における相互認証の成立を条件としてコンテンツの記録媒体に対する記録処理に伴う処理を実行する構成を有することを特徴とする。
【００２８】
さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、コンテンツの記録媒体に対する記録処理において、前記権利管理（ＤＲＭ）データの更新を実行した場合に、前記暗号処理手段において、該更新された権利管理（ＤＲＭ）データに基づく改竄チェック値（ＩＣＶ）を生成し、記録媒体に更新された権利管理（ＤＲＭ）データに基づく更新改竄チェック値（ＩＣＶ）を記録する構成であることを特徴とする。
【００３１】
さらに、本発明の第２の側面は、
記録媒体からのデータ再生処理を実行する情報再生装置において、
記録媒体に格納されたコンテンツの復号処理を実行するとともに、コンテンツの利用制限情報を含むコンテンツの権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）の検証を実行する暗号処理手段と、
前記記録媒体の物理的保護領域からの前記改竄チェック値（ＩＣＶ）の再生処理に適用し、前記暗号化コンテンツの再生処理には適用することのない秘密情報再生専用回路を有し、
前記暗号処理手段は、
階層ツリー構造におけるリーフを構成する選択された情報再生装置においてのみ復号可能な有効化キーブロック（ＥＫＢ）の復号処理によって取得されるＥＫＢキーを適用して、前記権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）の生成に適用するＩＣＶキーを生成し、生成したＩＣＶキーを適用して前記権利管理（ＤＲＭ）データの改竄チェック処理を実行し、改竄無しの確認を条件として、前記ＥＫＢキーを適用してコンテンツ復号に適用する暗号化コンテンツキーの復号を実行してコンテンツキーを生成し、生成したコンテンツキーにより、暗号化コンテンツの復号処理を行うことを特徴とする情報再生装置にある。
【００３２】
さらに、本発明の情報再生装置の一実施態様において、前記権利管理（ＤＲＭ）データは、コンテンツの利用に関する情報、コンテンツの暗号化キーとしてのコンテンツキーを暗号化した暗号化コンテンツキー、およびコンテンツ識別子（ＩＤ）を含むものであることを特徴とする。
【００３３】
さらに、本発明の情報再生装置の一実施態様において、前記秘密情報再生専用回路は、前記コンテンツの再生方式に適用する信号処理と異なる信号処理を適用して前記改竄チェック値（ＩＣＶ）の前記記録媒体の物理的保護領域からの再生処理を実行する構成を有することを特徴とする。
【００３４】
さらに、本発明の情報再生装置の一実施態様において、前記秘密情報再生専用回路は、前記コンテンツの再生方式に適用する信号処理と異なる信号処理を適用して前記改竄チェック値（ＩＣＶ）の前記記録媒体の物理的保護領域からの再生処理を実行する構成を有するとともに、前記秘密情報再生専用回路は、前記改竄チェック値（ＩＣＶ）を含む秘密情報を、対応コンテンツの記録媒体における記録領域に重畳する領域から再生する処理を実行する構成を有することを特徴とする。
【００５２】
さらに、本発明の第３の側面は、
情報記録装置において、記録媒体に対するデータ記録処理を実行する情報記録方法であり、

暗号処理手段が、記録媒体に格納するコンテンツの暗号化処理を実行し暗号化コンテンツを生成するとともに、コンテンツの利用制限情報を含むコンテンツの権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）を生成する暗号処理ステップと、
記録部が、記録媒体に対するデータ記録処理を実行する記録ステップを有し、
前記暗号処理ステップは、
階層ツリー構造におけるリーフを構成する選択された情報記録装置においてのみ復号可能な有効化キーブロック（ＥＫＢ）の復号処理によって取得されるＥＫＢキーを適用して、前記権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）の生成に適用するＩＣＶキーを生成し、さらに、前記ＥＫＢキーを適用してコンテンツ暗号化に適用するコンテンツキーの暗号化を実行して暗号化コンテンツキーを生成するステップであり、
前記記録ステップは、
前記暗号化コンテンツと、前記有効化キーブロック（ＥＫＢ）と、前記暗号化コンテンツキー、および前記権利管理（ＤＲＭ）データを通常のデータ記録再生処理の適用領域であるユーザ領域に記録し、
前記改竄チェック値（ＩＣＶ）を、専用回路によってのみ記録再生が可能な保護領域に記録するステップであることを特徴とする情報記録方法にある。

【００６７】

さらに、本発明の第４の側面は、
情報再生装置において、記録媒体からのデータ再生処理を実行する情報再生方法であり、
暗号処理手段が、記録媒体に格納されたコンテンツの復号処理を実行するとともに、コンテンツの利用制限情報を含むコンテンツの権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）の検証を実行する暗号処理ステップと、
再生手段が、記録媒体からのデータ再生処理を実行する再生ステップを有し、
前記暗号処理ステップは、
階層ツリー構造におけるリーフを構成する選択された情報再生装置においてのみ復号可能な有効化キーブロック（ＥＫＢ）の復号処理によって取得されるＥＫＢキーを適用して、前記権利管理（ＤＲＭ）データの改竄チェック値（ＩＣＶ）の生成に適用するＩＣＶキーを生成し、生成したＩＣＶキーを適用して前記権利管理（ＤＲＭ）データの改竄チェック処理を実行し、改竄無しの確認を条件として、前記ＥＫＢキーを適用してコンテンツ復号に適用する暗号化コンテンツキーの復号を実行してコンテンツキーを生成し、生成したコンテンツキーにより、暗号化コンテンツの復号処理を行うステップを含むことを特徴とする情報再生方法にある。

【００８４】

なお、本発明のプログラム記憶媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【００８５】

このようなプログラム記憶媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと記憶媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該記憶媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【００８６】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００８７】

【発明の実施の形態】

［デバイス構成］
図１に、音楽データ、画像データなどのコンテンツ利用デバイスの一例として、記録再生装置１００の構成を示すブロック図を示す。記録再生装置１００には例えばＰＣ、音楽記録再生装置、画像記録再生装置など、据え置き型、携帯型の装置が含まれる。なお、以下の説明では、記録再生両機能を持つ装置を代表して説明するが、記録のみ、あるいは再生のみの機能を持つ装置についても、本発明の構成の適用が可能である。
【００８８】
図１の装置について説明する。記録再生装置１００は、入出力Ｉ／Ｆ(Interface)１２０、コーデック１３０、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を備えた入出力Ｉ／Ｆ(Interface)１４０、暗号処理手段１５０、ＲＯＭ（Read Only Memory）１６０、ＣＰＵ(Central Processing Unit)１７０、ＲＡＭ１８０、記録媒体（メディア）のインタフェースとしてのメディアインタフェース１９０を有し、これらはバス１１０によって相互に接続されている。
【００８９】
入出力Ｉ／Ｆ１２０は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス１１０上に出力するとともに、バス１１０上のデジタル信号を受信し、外部に出力する。コーデック１３０は、バス１１０を介して供給される例えば画像であれば符号化（ｅｘ．ＭＰＥＧ符号化）されたデータをデコードし、入出力Ｉ／Ｆ１４０に出力するとともに、入出力Ｉ／Ｆ１４０から供給されるデジタル信号をエンコードしてバス１１０上に出力する。音声データであれば、ＡＴＲＡＣ３やＭＰ３などの形で圧縮、あるいはリニアＰＣＭ（linear PCM）での符号化されたデータを、デコードし、入出力Ｉ／Ｆ１４０に出力するとともに、入出力Ｉ／Ｆ１４０から供給されるデジタル信号をエンコードしてバス上に出力する。
【００９０】
入出力Ｉ／Ｆ１４０は、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を内蔵している。入出力Ｉ／Ｆ１４０は、外部から供給されるコンテンツとしてのアナログ信号を受信し、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ(Analog Digital)変換することで、デジタル信号として、コーデック１３０に出力するとともに、コーデック１３０からのデジタル信号を、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ(Digital Analog)変換することで、アナログ信号として、外部に出力する。
【００９１】
暗号処理手段１５０は、例えば、１チップＬＳＩ(Large Scale Integrated Circuit)で構成され、バス１１０を介して供給されるコンテンツとしてのデジタル信号の暗号化、復号処理、あるいは認証処理を実行し、暗号データ、復号データ等をバス１１０上に出力する構成を持つ。なお、暗号処理手段１５０は１チップＬＳＩに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。
【００９２】
ＲＯＭ１６０は、記録再生装置によって処理されるプログラムデータを格納する。ＣＰＵ１７０は、ＲＯＭ１６０、ＲＡＭ１８０に記憶されたプログラムを実行することで、コーデック１３０や暗号処理手段１５０等を制御する。ＲＡＭ１８０は、例えば、不揮発性メモリで、ＣＰＵ１７０が実行するプログラムや、ＣＰＵ１７０の動作上必要なデータ、さらにデバイスによって実行される暗号処理に使用されるキーセットを記憶する。キーセットについては後段で説明する。メディアインタフェース１９０は、デジタルデータを記録再生可能なメディア（記録媒体）を駆動することにより、記録媒体からデジタルデータを読み出し（再生し）、バス１１０上に出力するとともに、バス１１０を介して供給されるデジタルデータを、メディア（記録媒体）に供給して記録させる。
【００９３】
なお、ここでのメディア（記録媒体）は、例えば、ＤＶＤ、ＣＤ等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはＲＡＭ等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、記録再生装置１００に対して着脱可能な構成、あるいは内

蔵する構成の両者を含むものである。

【００９４】

メディアに記録されるコンテンツは暗号化により保護される。暗号を解く鍵はメディア上にコンテンツとともに、安全な方法で記録され、そのコンテンツの識別子（ＩＤ）およびそのコンテンツの利用形態についてののルールを表す権利データ（rights data）とともに改竄チェック値（ＩＣＶ：Integrity Check Value）による正当性が保証された形で記録される。権利データ（rights data）は、例えば再生許容回数：Ｎ回、コピー許容回数：Ｎ回、世代間コピー許容世代数：Ｎなど、コンテンツの再生、コピーなどのコンテンツ利用に関するルールを記録している。改竄チェック値（ＩＣＶ）およびＩＣＶを生成するための鍵データはメディア上に物理的に保護されて記録される。すなわち、通常のユーザデータ（コンテンツ）の記録再生方法での記録再生ができない保護データとして記録される。改竄チェック値（ＩＣＶ：Integrity Check Value）の生成、ＩＣＶを利用した改竄検証方法については後述する。

【００９５】

改竄チェック値（ＩＣＶ）およびＩＣＶを生成するための鍵データ等の秘密データは、通常のコンテンツ記録再生とは別な方法を使用した場合にのみ記録再生可能となる。この秘密データ格納領域に記録された保護データは正当なデバイスのみに装着された秘密情報記録再生専用回路としてのＩＣを利用した処理によって再生可能であり、また記録可能である。図１のメディアインタフェース１９０内のＩＣ１９５は、この秘密データの記録再生処理専用ＩＣである。正当なデバイスにのみＩＣ１９５が装着されユーザに提供されることになる。

【００９６】

［改竄チェック値（ＩＣＶ:Integrity Check Value）］

次に、データの改竄を防止するためのインテグリティ（改竄）・チェック値（ＩＣＶ）について説明する。

【００９７】

インテグリティ・チェック値（ＩＣＶ）は、改竄防止データとして、例えばコンテンツ、コピー制御情報等に対して生成され、ＩＣＶに基づいてこれら対象データの改竄検証が実行される。本発明のシステムにおいてはインテグリティ・チェック値（ＩＣＶ）は、上述した権利データ（rights data）、コンテンツＩＤ、および暗号化されたコンテンツキーの集合体としてのＤＲＭ（Digital Rights Management：デジタル権利管理）データを対象として生成され、このコンテンツの権利管理（ＤＲＭ）データの改竄の有無が検証される。

【００９８】

ＤＥＳ暗号処理構成を用いた改竄チェック値（ＩＣＶ）生成例を図２に示す。図２の構成に示すように対象となる改竄チェックデータを構成するメッセージを８バイト単位に分割（以下、分割されたメッセージをＤ０、Ｄ１、Ｄ２、・・・、Ｄｎ－１とする）する。改竄チェックデータは、例えば上述の権利管理（ＤＲＭ：Digital Rights Management）データである。

【００９９】

まず、初期値（Initial Value（以下、ＩＶとする））とＤ０を排他的論理和する（その結果をＩ１とする）。なお、ここでは、初期値ＩＶを用いた処理について説明するが、初期値ＩＶを用いない構成（ex.ISO9797,DES-MAC）としてもよい。初期値ＩＶを用いることでシステム全体の安全性を高めることが可能となるが、ＩＣＶ、ＩＣＶキーとともに初期値ＩＶも安全な方法で管理する必要がある。次に、Ｉ１をＤＥＳ暗号化部に入れ、改竄チェック値（ＩＣＶ）生成鍵（ＩＣＶ生成検証キー：Ｋｉｃｖ）を用いて暗号化する（出力をＥ１とする）。続けて、Ｅ１およびＤ１を排他的論理和し、その出力Ｉ２をＤＥＳ暗号化部へ入れ、改竄チェック値（ＩＣＶ）生成鍵（ＩＣＶ生成検証キー：Ｋｉｃｖ）を用いて暗号化する（出力Ｅ２）。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたＥＮをＤＲＭチェック値ＩＣＶ’とする。

【０１００】
改竄のないことが保証された例えばＤＲＭ生成時に生成した正当なＩＣＶと、新たにＤＲＭに基づいて生成したＩＣＶ’とを比較して同一性が立証、すなわちＩＣＶ’＝ＩＣＶであれば入力メッセージ、ここでは権利データ（rights data）、コンテンツＩＤ、暗号化されたコンテンツキーの集合体としての権利管理（ＤＲＭ：Digital Rights Management）データに改竄のないことが保証され、ＩＣＶ’≠ＩＣＶであれば改竄があったと判定される。
【０１０１】
ＩＣＶを使用したデータ改竄チェック処理フローを図３に示す。まず、改竄チェックの対象データを抽出し（Ｓ１１）、抽出したデータに基づいて例えば図２のＤＥＳ暗号処理構成によりＩＣＶ’を計算する（Ｓ１２）。計算の結果、算出されたＩＣＶ’とデータ内に格納されたＩＣＶとを比較し（Ｓ１３）、一致した場合は、データの改竄が無く正当なデータであると判定（Ｓ１４からＳ１５）され、不一致の場合は、データの改竄があると判定（Ｓ１４からＳ１６）される。
【０１０２】
［キー配信構成としてのツリー（木）構造について］
本発明のシステムにおいては、図１に示す記録再生装置等のコンテンツ利用を行なう各デバイスはキー配信構成としてのツリー（木）構造に基づく暗号処理鍵を保有する。ツリー（木）構造に基づくキー配信構成を図４を用いて説明する。
【０１０３】
図４の最下段に示すナンバ０～１５がコンテンツ利用側の個々のデバイスである。すなわち図４に示す階層ツリー（木）構造の各葉(リーフ：leaf)がそれぞれのデバイスに相当する。
【０１０４】
各デバイス０～１５は、製造時あるいは出荷時、あるいはその後において、図４に示す階層ツリー（木）構造における、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーからなるキーセットをメモリに格納する。図４の最下段に示すＫ０００００～Ｋ１１１１が各デバイス０～１５にそれぞれ割り当てられたリーフキーであり、最上段のＫＲ（ルートキー）から、最下段から２番目の節（ノード）に記載されたキー：ＫＲ～Ｋ１１１をノードキーとする。
【０１０５】
図４に示すツリー構成において、例えばデバイス０はリーフキーＫ００００と、ノードキー：Ｋ０００、Ｋ００、Ｋ０、ＫＲを所有する。デバイス５はＫ０１０１、Ｋ０１０、Ｋ０１、Ｋ０、ＫＲを所有する。デバイス１５は、Ｋ１１１１、Ｋ１１１、Ｋ１１、Ｋ１、ＫＲを所有する。なお、図４のツリーにはデバイスが０～１５の１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。
【０１０６】
また、図４のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたＤＶＤ、ＣＤ、ＭＤ、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図４に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。
【０１０７】
これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図４の点線で囲んだ部分、すなわちデバイス０，１，２，３を同一の記録媒体を用いる１つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、各デバイス

共通に使用するコンテンツ暗号化または復号キーとしてのコンテンツキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図４の点線で囲んだ部分、すなわちデバイス０，１，２，３を１つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図３のツリー中に複数存在する。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、メッセージデータ配信手段として機能する。

【０１０８】

なお、ノードキー、リーフキーは、ある１つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【０１０９】

このツリー構造において、図４から明らかなように、１つのグループに含まれる３つのデバイス０，１，２，３はノードキーとして共通のキーＫ００、Ｋ０、ＫＲを保有する。このノードキー共有構成を利用することにより、例えば共通のコンテンツキーをデバイス０，１，２，３のみに提供することが可能となる。たとえば、共通に保有するノードキーＫ００自体をコンテンツキーとして設定すれば、新たな鍵送付を実行することなくデバイス０，１，２，３のみが共通のコンテンツキーの設定が可能である。また、新たなコンテンツキーＫｃｏｎをノードキーＫ００で暗号化した値Ｅｎｃ（Ｋ００，Ｋｃｏｎ）を、ネットワークを介してあるいは記録媒体に格納してデバイス０，１，２，３に配布すれば、デバイス０，１，２，３のみが、それぞれのデバイスにおいて保有する共有ノードキーＫ００を用いて暗号Ｅｎｃ（Ｋ００，Ｋｃｏｎ）を解いてコンテンツキー：Ｋｃｏｎを得ることが可能となる。なお、Ｅｎｃ（Ｋａ，Ｋｂ）はＫｂをＫａによって暗号化したデータであることを示す。

【０１１０】

また、ある時点ｔにおいて、デバイス３の所有する鍵：Ｋ００１１,Ｋ００１,Ｋ００,Ｋ０,ＫＲが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキー：Ｋ００１，Ｋ００,Ｋ０,ＫＲをそれぞれ新たな鍵Ｋ（ｔ）００１,Ｋ（ｔ）００,Ｋ（ｔ）０,Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）：ｔの更新キーであることを示す。

【０１１１】

更新キーの配布処理ついて説明する。キーの更新は、例えば、図５（Ａ）に示す有効化キーブロック（ＥＫＢ：Enabling Key Block）と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス０，１，２に供給することによって実行される。なお、有効化キーブロック（ＥＫＢ）は、図４に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化キーによって構成される。

【０１１２】

図５（Ａ）に示す有効化キーブロック（ＥＫＢ）には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図５の例は、図４に示すツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布することを目的として形成されたブロックデータである。図４から明らかなように、デバイス０，デバイス１は、更新ノードキーとしてＫ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要であり、デバイス２は、更新ノードキーとしてＫ（ｔ）００１、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要である。

【０１１３】
図５（Ａ）のＥＫＢに示されるようにＥＫＢには複数の暗号化キーが含まれる。最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自身の持つリーフキーによってこの暗号化キーを復号し、Ｋ（ｔ）００１を得ることができる。また、復号により得たＫ（ｔ）００１を用いて、図５（Ａ）の下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）を復号可能となり、更新ノードキーＫ（ｔ）００を得ることができる。以下順次、図５（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図５（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。一方、デバイスＫ００００．Ｋ０００１は、ノードキーＫ０００は更新する対象に含まれておらず、更新ノードキーとして必要なのは、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒである。デバイスＫ００００．Ｋ０００１は、図５（Ａ）の上から３段目の暗号化キーＥｎｃ（Ｋ０００，Ｋ（ｔ）００）を復号しＫ（ｔ）００、を取得し、以下、図５（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図５（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。このようにして、デバイス０，１，２は更新した鍵Ｋ（ｔ）００１,Ｋ（ｔ）００,Ｋ（ｔ）０,Ｋ（ｔ）Ｒを得ることができる。なお、図５（Ａ）のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【０１１４】
図４に示すツリー構造の上位段のノードキー：Ｋ（ｔ）０,Ｋ（ｔ）Ｒの更新が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図５（Ｂ）の有効化キーブロック（ＥＫＢ）を用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

【０１１５】
図５（Ｂ）に示すＥＫＢは、例えば特定のグループにおいて共有する新たなコンテンツキーを配布する場合に利用可能である。具体例として、図４に点線で示すグループ内のデバイス０，１，２，３がある記録媒体を用いており、新たな共通のコンテンツキーＫ（ｔ）ｃｏｎが必要であるとする。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００を用いて新たな共通の更新コンテンツキー：Ｋ（ｔ）ｃｏｎを暗号化したデータＥｎｃ（Ｋ（ｔ），Ｋ（ｔ）ｃｏｎ）を図５（Ｂ）に示すＥＫＢとともに配布する。この配布により、デバイス４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

【０１１６】
すなわち、デバイス０，１，２はＥＫＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号すれば、ｔ時点でのコンテンツキーＫ（ｔ）ｃｏｎを得ることが可能になる。

【０１１７】
［ＥＫＢを使用したキーの配布］
図６に、ｔ時点でのコンテンツキーＫ（ｔ）ｃｏｎを得る処理例として、Ｋ（ｔ）００を用いて新たな共通のコンテンツキーＫ（ｔ）ｃｏｎを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｃｏｎ）と図５（Ｂ）に示すＥＫＢとを記録媒体を介して受領したデバイス０の処理を示す。すなわちＥＫＢによる暗号化メッセージデータをコンテンツキーＫ（ｔ）ｃｏｎとした例である。

【０１１８】
図６に示すように、デバイス０は、記録媒体に格納されている世代：t時点のＥＫＢと自分があらかじめ格納しているノードキーＫ０００を用いて上述したと同様のＥＫＢ処理により、ノードキーＫ（ｔ）００を生成する。さらに、復号した更新ノードキーＫ（ｔ）００を用いて更新コンテンツキーＫ（ｔ）ｃｏｎを復号して、後にそれを使用するために自分だけが持つリーフキーＫ００００で暗号化して格納する。

【０１１９】
［ＥＫＢのフォーマット］
図７に有効化キーブロック（ＥＫＢ）のフォーマット例を示す。バージョン２０１は、有効化キーブロック（ＥＫＢ）のバージョンを示す識別子である。なお、バージョンは最新のＥＫＢを識別する機能とコンテンツとの対応関係を示す機能を持つ。デプスは、有効化キーブロック（ＥＫＢ）の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ２０３は、有効化キーブロック（ＥＫＢ）中のデータ部の位置を示すポインタであり、タグポインタ２０４はタグ部の位置、署名ポインタ２０５は署名の位置を示すポインタである。
【０１２０】
データ部２０６は、例えば更新するノードキーを暗号化したデータを格納する。例えば図６に示すような更新されたノードキーに関する各暗号化キー等を格納する。
【０１２１】
タグ部２０７は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図８を用いて説明する。図８では、データとして先に図５（Ａ）で説明した有効化キーブロック（ＥＫＢ）を送付する例を示している。この時のデータは、図８の表（ｂ）に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キーＫ（ｔ）Ｒが含まれているので、トップノードアドレスはＫＲとなる。このとき、例えば最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）は、図８の（ａ）に示す階層ツリーに示す位置にある。ここで、次のデータは、Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが０、ない場合は１が設定される。タグは｛左（Ｌ）タグ，右（Ｒ）タグ｝として設定される。最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）の左にはデータがあるので、Ｌタグ＝０、右にはデータがないので、Ｒタグ＝１となる。以下、すべてのデータにタグが設定され、図８（ｃ）に示すデータ列、およびタグ列が構成される。
【０１２２】
タグは、データＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）がツリー構造のどこに位置しているのかを示すために設定されるものである。データ部に格納されるキーデータＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）．．．は、単純に暗号化されたキーの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化キーのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図５で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、
０：Ｅｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）ｒｏｏｔ）
００：Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）
０００：Ｅｎｃ（Ｋ（（ｔ）０００，Ｋ（Ｔ）００）
．．．のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。
【０１２３】
図７に戻って、ＥＫＢフォーマットについてさらに説明する。署名（Signature）は、有効化キーブロック（ＥＫＢ）を発行した例えば鍵管理センタ、コンテンツロバイダ、決済機関等が実行する電子署名である。ＥＫＢを受領したデバイスは署名検証によって正当な有効化キーブロック（ＥＫＢ）発行者が発行した有効化キーブロック（ＥＫＢ）であることを確認する。
【０１２４】
図９にコンテンツキー暗号キーＫＥＫを、図４に示すノードキーＫ００を更新した更新ノードキーＫ（ｔ）００として構成した場合の例を示す。この場合、図４の点線枠で囲んだグループにおいてデバイス３が、例えば鍵の漏洩によりリボーク（排除）されているとし

て、他のグループのメンバ、すなわち、デバイス０，１，２に対して図９に示す（ａ）有効化キーブロック（ＥＫＢ）と、（ｂ）コンテンツキー（Ｋｃｏｎ）をコンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）で暗号化したデータと、（ｃ）コンテンツ（content）をコンテンツキー（Ｋｃｏｎ）で暗号化したデータとを配信することにより、デバイス０，１，２はコンテンツを得ることができる。

【０１２５】

図９の右側には、デバイス０における復号手順を示してある。デバイス０は、まず、受領した有効化キーブロックから自身の保有するリーフキーＫ０００を用いた復号処理により、コンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）を取得する。次に、Ｋ（ｔ）００による復号によりコンテンツキーＫｃｏｎを取得し、さらにコンテンツキーＫｃｏｎによりコンテンツの復号を行なう。これらの処理により、デバイス０はコンテンツを利用可能となる。デバイス１，２においても各々異なる処理手順でＥＫＢを処理することにより、コンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）を取得することが可能となり、同様にコンテンツを利用することが可能となる。

【０１２６】

図４に示す他のグループのデバイス４，５，６…は、この同様のデータ（ＥＫＢ）を受信したとしても、自身の保有するリーフキー、ノードキーを用いてコンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）を取得することができない。同様にリボークされたデバイス３においても、自身の保有するリーフキー、ノードキーでは、コンテンツキー暗号キー（ＫＥＫ＝Ｋ（ｔ）００）を取得することができず、正当な権利を有するデバイスのみがコンテンツを復号して利用することが可能となる。

【０１２７】

このように、ＥＫＢを利用したコンテンツキーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能とした暗号化コンテンツを配信することが可能となる。

【０１２８】

なお、有効化キーブロック（ＥＫＢ）、コンテンツキー、暗号化コンテンツ等は、ネットワークを介して安全に配信することが可能な構成であるが、有効化キーブロック（ＥＫＢ）、コンテンツキー、暗号化コンテンツをＤＶＤ、ＣＤ等の記録媒体に格納してユーザに提供することも可能である。この場合、記録媒体に格納された暗号化コンテンツの復号には、同一の記録媒体に格納された有効化キーブロック（ＥＫＢ）の復号により得られるコンテンツキーを使用するように構成すれば、予め正当権利者のみが保有するリーフキー、ノードキーによってのみ利用可能な暗号化コンテンツの配布処理、すなわち利用可能なユーザデバイスを限定したコンテンツ配布が簡易な構成で実現可能となる。

【０１２９】

図１に示す記録再生装置などのデバイスは、上述の有効化キーブロック（ＥＫＢ）の処理（復号）を行なうためのリーフキー、ノードキーからなるキーセットを格納し、必要に応じて格納されたキーセットを用いて有効化キーブロック（ＥＫＢ）の処理を実行し、ＥＫＢ配信されたキー（ｅｘ．ルートキー、キー暗号キー（ＫＥＫ））を取得する。

【０１３０】

[メディア（記録媒体）]

次に、本発明のシステムにおいて用いられるデジタルデータを記録するＣＤ、ＤＶＤなどのメディアについて説明する。

【０１３１】

メディア上の領域はユーザ領域と保護領域とに区別される。ユーザ領域は、通常のコンテンツの記録再生方式に従った記録再生が可能な領域であり、保護領域は、通常のコンテンツの記録再生方式と異なる方式によってのみ記録再生可能な領域である。この保護領域は、前述の図１で説明した秘密情報記録再生専用回路としてのＩＣ１９５を用いてのみ記録再生が可能な領域である。なお、ここでユーザ領域と保護領域はメディア上において、記録領域の位置的な差異として区別される場合と、記録再生の信号処理方式の差異として区

別される場合の両者がある。

【０１３２】

ユーザ領域と保護領域とを記録領域の位置的な差異として区別する場合とは、保護領域を通常のコンテンツ記録再生領域として設定されていない例えば内周領域に設定する構成であり、ユーザ領域と保護領域とを信号処理方式の差異として区別する場合とは、保護領域のデータ記録再生を、通常のコンテンツ記録再生とは異なる信号処理を適用して実行する場合である。例えばＣＤにおいて、コンテンツデータは、メディア上にピット（pit）とランド（land）として記録されるが、このときのデータ信号の直流成分が極小になるように、ＥＦＭ信号を付加する。ＥＦＭ信号の付加方法はＣＤ記録における信号変調方式で決められており、この信号はコマンドなどにより操作することはできない。このＥＦＭ信号を前述の秘密情報記録再生専用回路としてのＩＣ１９５によりコントロールすることにより秘密情報の保護領域に対する記録再生を行なう。この秘密データ部分は、通常のコンテンツ記録再生方法では記録再生が出来ず、前述のＩＣ１９５を通してのみ記録再生が可能となる。

【０１３３】

保護領域とを記録領域の位置的な差異として区別する場合、信号処理方式の差異として区別する場合、いずれの場合も、保護領域に対するデータの記録再生は、ＩＣ１９５を用いてのみ実行可能となる。

【０１３４】

メディアのデータ構成を図１０を用いて説明する。通常のデータ記録エリアであるユーザ領域（user area）３２０にはコンテンツ（Contents）に対応した有効化キーブロック（ＥＫＢ）３２１と、コンテンツキー３２５によって暗号化されたコンテンツ（contents）３２３、前述の有効化キーブロック（ＥＫＢ）の復号処理によって得られるＥＫＢキー（ｅｘ．ルートキー、キー暗号キー（ＫＥＫ））３２４によって暗号化されたコンテンツキー３２２、および、コンテンツ利用方法についてのルール、例えばコピー可、不可などの利用制限情報としての権利データを含む前述したＤＲＭデータ３２６が記録される。

【０１３５】

秘密情報の記録エリアである保護領域（protected area）３１０には、ＤＲＭデータの改竄（Integrity）を検証するのに用いられる前述したＩＣＶ生成検証キーの元データとして利用されるＩＣＶキー３１１、およびＤＲＭデータにＩＣＶ生成検証キーを作用させて生成したインテグリティ（改竄）・チェック値（ＩＣＶ）３１２が記録される。

【０１３６】

［オーサリング・デバイス］

次に、暗号化コンテンツを格納したデバイスを製造するオーサリング・デバイスの構成について図１１を用いて説明する。

【０１３７】

図１１の装置について説明する。オーサリングデバイス４００は、入出力Ｉ／Ｆ(Interface)４２０、暗号処理手段４５０、ＲＯＭ（Read Only Memory）４６０、ＣＰＵ(Central Processing Unit)４７０、ＲＡＭ４８０、記録媒体（メディア）のインタフェースとしてのメディアインタフェース４９０を有し、これらはバス４１０によって相互に接続されている。

【０１３８】

入出力Ｉ／Ｆ４２０は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス４１０上に出力する。

【０１３９】

暗号処理手段４５０は、例えば、１チップＬＳＩ(Large Scale Integrated Circuit)で構成され、バス４１０を介して供給されるコンテンツとしてのデジタル信号の暗号化を実行し、暗号データをバス４１０上に出力する構成を持つ。なお、暗号処理手段４５０は１チップＬＳＩに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。

【０１４０】
ＲＯＭ４６０は、オーサリングデバイスによって処理されるプログラムデータを格納する。ＣＰＵ４７０は、ＲＯＭ４６０、ＲＡＭ４８０に記憶されたプログラムを実行することで、暗号処理手段４５０等を制御する。ＲＡＭ４８０は、例えば、不揮発性メモリで、ＣＰＵ４７０が実行するプログラムや、ＣＰＵ４７０の動作上必要なデータ、さらに暗号処理に使用されるキーデータなどを記憶する。メディアインタフェース４９０は、デジタルデータを記録再生可能なメディア（記録媒体）を駆動することにより、バス４１０を介して供給されるデジタルデータを、メディア（記録媒体）に供給して記録させる。
【０１４１】
なお、ここでのメディア（記録媒体）は、例えば、ＤＶＤ、ＣＤ等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはＲＡＭ等の半導体メモリ等のデジタルデータの記憶可能な媒体である。なお、ＣＤ、ＤＶＤなど、同一のコンテンツ記録媒体を多数製造する際には、オーサリングデバイスにおいて原盤を作成し、その後メディアスタンパを使用して、同一データの記録されたＣＤ、ＤＶＤなどを生産する。
【０１４２】
オーサリングデバイスにおけるデジタルコンテンツの暗号化およびメディアに対する記録処理について説明する。オーサリングデバイスは、まず、暗号化されていないデジタルコンテンツ、そのコンテンツのプロテクション、すなわち暗号化処理に用いるＥＫＢキー（ｅｘ．ルートキー、キー暗号キー（ＫＥＫ））を含むＥＫＢを受け取る。ＥＫＢは信頼できる鍵管理センターＫＤＣ(Key Distribution Center)から発行される。
【０１４３】
鍵管理センターＫＤＣ(Key Distribution Center)は、コンテンツプロバイダ（Contents Provider）が生成したコンテンツキーの暗号化キーとしての例えばルートキーを正当なユーザデバイスのみにおいて復号可能としたＥＫＢを生成する。なお、鍵管理センターＫＤＣ(Key Distribution Center)は、各デバイス（device）の格納キーセットを直接知ることなく、デバイス（device）を管理するエンティティからの情報に基づいて正当なユーザデバイスのみが復号可能なＥＫＢを生成することが可能である。
【０１４４】
コンテンツプロバイダ（Contents Provider）であるオーサリング・エンティティ（Authoring Entity）は、コピー許容回数などの利用制限情報からなるコンテンツに付加する権利データ（Rights data）と、コンテンツの識別子（ＩＤ）を受け取り、それらのデータからメディアに記録されるデータを生成する。ＤＲＭデータに対して付加する改竄チェック値（ＩＣＶ）は、同一コンテンツを記録したメディアについては、そのコンテンツで同一、またはスタンパ毎に同一であってよく、メディア毎に異なる必要はない。すなわち、同一のＩＣＶキーおよびＥＫＢを用いて生成されたＩＣＶでもよい。
【０１４５】
図１２にオーサリングデバイスによるコンテンツの暗号化およびメディアに対する記録処理を説明するブロック図を示す。
【０１４６】
オーサリングデバイス４００は、書き込みデータ生成処理および、メディア５００に対するメディア書き込み処理を実行する。図１２に示すように、メディアに書き込むデータは、ユーザ領域に対してはＥＫＢ、ＤＲＭデータ（権利データ、コンテンツＩＤ、暗号化コンテンツキー）、および暗号化コンテンツである。また保護領域に対しては、ＩＣＶ生成検証キーの元データであるＩＣＶキーと、ＤＲＭデータに対してＩＣＶ生成検証キーを作用させて生成した改竄チェック値（ＩＣＶ）である。各データの生成、記録処理について説明する。
【０１４７】
ａ．ＥＫＢ
ＥＫＢは、正当なライセンス、すなわちメデイアに対して記録するコンテンツを正当に利用する権利を持つユーザによってのみ復号可能なＥＫＢであり、前述したように鍵管理セ

ンターＫＤＣ(Key Distribution Center)によって発行される。このＥＫＢは、メディア５００のユーザ領域に記録される。

【０１４８】

ｂ．ＩＣＶキー

ＩＣＶキーは、乱数発生装置などのキー・ジェネレータ４２１によって生成され、生成されたＩＣＶキーは、メディア５００の保護領域に格納される。なお、保護領域へのデータ書き込みは、メディアインタフェース４２４内の秘密情報記録再生専用回路としての専用ＩＣ４２５による処理、すなわち特定領域への書き込み処理、あるいは特定信号処理方式として実行される。

【０１４９】

ｃ．ＩＣＶ

ＩＣＶは、ＤＲＭデータ（権利データ、コンテンツＩＤ、暗号化コンテンツキー）に対してＩＣＶ生成検証キーを作用させて生成される改竄チェック値であり、前述した図２の処理構成によって生成される。ＩＣＶ生成検証キーは、図１２の鍵生成部（Ｆｕｎｃ）４２２において、キー・ジェネレータ４２１によって生成されたＩＣＶキーにＥＫＢキー（ｅｘ．ルートキー、キー暗号キー（ＫＥＫ））を作用（ｅｘ．ＤＥＳ暗号化処理）させて生成されるキーである。オーサリングデバイスは、ＤＲＭデータを構成する権利データと、コンテンツ識別子を入力し、さらに、暗号化コンテンツキーを加えてＤＲＭデータを生成する。暗号化コンテンツキーは、キー・ジェネレータ４１１で生成したコンテツキー（Ｋｃ）をＥＫＢキー（ｅｘ．ルートキー、キー暗号キー（ＫＥＫ））で暗号処理部（Ｅｎｃ）４１２で暗号化して生成する。

【０１５０】

このようにして生成した暗号化コンテンツキーと、権利データ、コンテンツＩＤを含むＤＲＭデータに対して、ＩＣＶ生成検証キーを作用させて前述の図２の構成に従ってＩＣＶ生成手段（Calculate ICV）４２３において改竄チェック値（ＩＣＶ）が生成されて、生成されたＩＣＶがメディア５００の保護領域に格納される。なお、保護領域へのデータ書き込みは、メディアインタフェース４２４内の秘密情報記録再生専用回路としての専用ＩＣ４２５による処理、すなわち特定領域への書き込み処理、あるいは特定信号処理方式として実行される。

【０１５１】

ｄ．ＤＲＭデータ

権利データ、コンテンツＩＤ、暗号化コンテンツキーから構成されるＤＲＭデータは、上述のＩＣＶ生成手段（Calculate ICV）４２３に対して入力されるデータであり、この入力データと同一のＤＲＭデータがメディア５００のユーザ領域に書き込まれる。このＤＲＭデータは、通常の記録再生処理によって記録再生可能なユーザ領域に書き込まれる。

【０１５２】

ｅ．暗号化コンテンツ

暗号化コンテンツは、メディアに対して記録されるコンテンツをコンテンツキーによって暗号化したデータであり、キージェネレータ４１１で生成したコンテンツキーを用いて入力コンテンツを暗号処理部４１３において暗号化し、これをメディア５００のユーザ領域に書き込む。この暗号化コンテンツは、通常の記録再生処理によって記録再生可能なユーザ領域に書き込まれる。

【０１５３】

図１３にオーサリングデバイスによるコンテンツの暗号化およびメディアに対する記録処理を説明するフローを示す。各ステップについて説明する。

【０１５４】

まず、コンテンツキーの暗号化に適用するＥＫＢキー、正当なデバイスにおいて処理可能であり、処理によりＥＫＢキーを取得可能なＥＫＢ、記録コンテンツに対応する権利データ、コンテンツＩＤ、コンテンツを受信（Ｓ１０１）する。

【０１５５】

次に、キー・ジェネレータ４１１でコンテツキー（Ｋｃ）を生成（Ｓ１０２）し、生成したコンテンツキーをＥＫＢキーで暗号化（Ｓ１０３）する。

【０１５６】

さらに、生成した暗号化コンテンツキーと、権利データ、コンテンツＩＤに基づいてＤＲＭデータを生成（Ｓ１０４）し、コンテツキー（Ｋｃ）に基づいてコンテンツを暗号化を実行（Ｓ１０５）する。

【０１５７】

次に、キー・ジェネレータ４２１によってＩＣＶキーを生成（Ｓ１０６）し、図１２の鍵生成部（Ｆｕｎｃ）４２２において、キー・ジェネレータ４２１によって生成されたＩＣＶキーにＥＫＢキー（ｅｘ．ルートキー、キー暗号キー（ＫＥＫ））を作用（ｅｘ．ＤＥＳ暗号化処理）させてＩＣＶ生成検証キー（鍵１）を生成（Ｓ１０７）する。

【０１５８】

生成したＩＣＶ生成検証キー（鍵１）を、暗号化コンテンツキーと、権利データ、コンテンツＩＤを含むＤＲＭデータに対して作用させて前述の図２の構成に従ってＩＣＶ生成手段（Calculate ICV）４２３において改竄チェック値（ＩＣＶ）を生成（Ｓ１０８）する。

【０１５９】

このようにして、生成したＩＣＶキー、ＩＣＶをメディアの保護領域に記録し、またＥＫＢ、暗号化コンテンツ、ＤＲＭデータ（暗号化コンテンツキー、権利データ、コンテンツＩＤ）をメディアのユーザ領域に記録（Ｓ１０９）して処理を終了する。

【０１６０】

［記録装置におけるメディアに対するコンテンツ記録処理］

次に、ユーザデバイスにおいて、コンテンツの記録を行なうことができる記録装置におけるメディアに対するコンテンツ記録処理について説明する。ユーザデバイスとしての記録装置では、デジタル、またはアナログインタフェースを通してデバイスに入力されたコンテンツをメディア上に記録することができる。コンテンツは、コンテンツプロバイダから提供されたコンテンツ、あるいはユーザが他装置において生成、取得したコンテンツ（ｅｘ．自己録再）等である。

【０１６１】

コンテンツの記録の際には、コンテンツキーによって暗号化した暗号化コンテンツをメディアのユーザ領域に記録する。また、権利データ、コンテンツＩＤ、暗号化コンテンツキーから構成されるＤＲＭデータをユーザ領域に記録する。さらに、ＤＲＭデータに対する改竄チェック値（ＩＣＶ）と、改竄チェック値（ＩＣＶ）の生成検証のためのＩＣＶ生成検証キーを生成するめためのＩＣＶキーをメディアの保護領域に記録する。また、ＩＣＶ生成検証キーの生成、コンテンツキーの生成に用いるＥＫＢをメディアのユーザ領域に記録する。

【０１６２】

メディアに記録するＥＫＢは、例えばコンテンツプロバイダによってユーザデバイスに提供されたコンテンツのようにコンテンツにＥＫＢが付帯している場合は、その入力ＥＫＢを使用する。また、自己録再時のようにＥＫＢを持たないコンテンツを記録する際には、デバイスに格納された自己録再用ＥＫＢを用いる。なお、自己録再ＥＫＢは、予めデバイスに格納された有効化キーブロック（ＥＫＢ）であり、例えば特定のデバイスグループに格納されたキーセット（リーフキー、ノードキーからなるキーセット）を使用した場合にのみ復号処理可能なＥＫＢである。なお、このＥＫＢは例えばメディアにあらかじめ記憶されているものであってもよく、その場合は、そのメディアに記憶されるコンテンツは必ずメディアにあらかじめ記憶されているＥＫＢを用いるようにするといった適切な方法を用いればよい。なお、不正なデバイスの排除（リボケーション）処理を行なう場合は、バージョンが新しくなったＥＫＢをネットワークまたはメディアを介してユーザデバイスに提供する。

【０１６３】

図１４にデジタルデータの記録可能なユーザデバイスによるコンテンツの暗号化およびメディアに対する記録処理を説明するブロック図を示す。

【０１６４】

ユーザデバイス６００は、図１４に示すように、メディア７００に対して、ユーザ領域にＥＫＢ、ＤＲＭデータ（権利データ、コンテンツＩＤ、暗号化コンテンツキー）、および暗号化コンテンツを書き込み、保護領域に対して、ＩＣＶ生成検証キーの元データであるＩＣＶキーと、ＤＲＭデータに対してＩＣＶ生成検証キーを作用させて生成した改竄チェック値（ＩＣＶ）を書き込む処理を実行する。各データの生成、記録処理について説明する。なお、図１４には、デバイスの暗号処理手段６１０（図１における暗号処理手段１５０に相当する）について、処理シーケンスに従って処理部を機能的に分割して示してあるが、これらの様々な処理部が個別に存在することを示すものではなく、各処理は暗号処理手段６１０が実行するものであり、説明のために各機能をブロックとして分割して示しているにすぎないものである。

【０１６５】

なお、図１４のメディア７００の上段に示す要求ＥＫＢバージョン（Required EKB Version）７１０は、このメディア７００に対してコンテンツを記録する際に適用する最低のＥＫＢバージョンを示すデータであり、ユーザ領域に記録されている。デバイスは、まず、メディアに記録されたＥＫＢバージョンを読み取り、コンテンツの記録に適用するＥＫＢのバージョンとの比較を実行して適用ＥＫＢバージョンがメディアに記録されたバージョンより古くない場合にのみＥＫＢを適用したコンテンツ記録を行なうことができる。なお、この処理については、図１７の処理フローについての説明において、さらに説明する。ここでは、デバイスがすでに最新のＥＫＢを取得できたものとして各データの書き込み処理について説明する。

【０１６６】

ａ．ＥＫＢ

ＥＫＢは、正当なライセンス、すなわちメデイアに対して記録するコンテンツを正当に利用する権利を持つユーザによってのみ復号可能なＥＫＢであり、前述したように鍵管理センターＫＤＣ(Key Distribution Center)によって発行され、コンテンツに対応して設定されたＥＫＢ、あるいは自己録再用のＥＫＢとして自デバイスに予め格納されたＥＫＢである。このＥＫＢは、メディア７００のユーザ領域に記録される。

【０１６７】

ｂ．ＩＣＶキー

ＩＣＶキーは、乱数発生装置などのキー・ジェネレータ２，６２１によって生成され、生成されたＩＣＶキーは、メディア７００の保護領域に格納される。なお、保護領域へのデータ書き込みは、メディアインタフェース６２４内の秘密情報記録再生専用回路としての専用ＩＣ６２５による処理、すなわち特定領域への書き込み処理、あるいは特定信号処理方式として実行される。

【０１６８】

ｃ．ＩＣＶ

ＩＣＶは、ＤＲＭデータ（権利データ、コンテンツＩＤ、暗号化コンテンツキー）に対してＩＣＶ生成検証キーを作用させて生成される改竄チェック値であり、前述した図２の処理構成によって生成される。ＩＣＶ生成検証キーは、図１４の鍵生成部（Ｆｕｎｃ）６２２において、キー・ジェネレータ６２１によって生成されたＩＣＶキーにＥＫＢキー（ｅｘ．ルートキー、キー暗号キー（ＫＥＫ））を作用（ｅｘ．ＤＥＳ暗号化処理）させて生成されるキーである。ＥＫＢキーは、デバイスの有するキーセット（リーフキー、ノードキー）によって、ＥＫＢ処理部（Process ＥＫＢ）６１４においてＥＫＢを復号処理することによって取得（図６，図９参照）可能なキーである。ユーザデバイスは、ＥＫＢ処理部（Process ＥＫＢ）６１３においてＥＫＢを復号処理することで取得したＥＫＢキーによりＩＣＶキーを処理（ｅｘ．ＤＥＳ暗号化）することでＩＣＶ生成検証キーを生成する。

【０１６９】
また、ユーザデバイスは、ＤＲＭデータを構成する権利データと、コンテンツ識別子を入力し、さらに、暗号化コンテンツキーを加えてＤＲＭデータを生成する。暗号化コンテンツキーは、キー・ジェネレータ１，６１１で生成したコンテツキー（Ｋｃ）をＥＫＢキー（ｅｘ．ルートキー、キー暗号キー（ＫＥＫ））により、暗号処理部（Ｅｎｃ）６１２において暗号化して生成する。
【０１７０】
このようにして生成した暗号化コンテンツキーと、権利データ、コンテンツＩＤを含むＤＲＭデータに対して、ＩＣＶ生成検証キーを作用させて前述の図２の構成に従ってＩＣＶ生成手段（Calculate ICV）６２３において改竄チェック値（ＩＣＶ）が生成されて、生成されたＩＣＶがメディア７００の保護領域に格納される。なお、保護領域へのデータ書き込みは、メディアインタフェース６２４内の秘密情報記録再生専用回路としての専用ＩＣ６２５による処理、すなわち特定領域への書き込み処理、あるいは特定信号処理方式として実行される。
【０１７１】
ｄ．ＤＲＭデータ
権利データ、コンテンツＩＤ、暗号化コンテンツキーから構成されるＤＲＭデータは、上述のＩＣＶ生成手段（Calculate ICV）６２３に対して入力されるデータであり、この入力データと同一のＤＲＭデータがメディア７００のユーザ領域に書き込まれる。このＤＲＭデータは、通常の記録再生処理によって記録再生可能なユーザ領域に書き込まれる。
【０１７２】
ｅ．暗号化コンテンツ
暗号化コンテンツは、メディアに対して記録されるコンテンツをコンテンツキーによって暗号化したデータであり、キージェネレータ１，６１１で生成したコンテンツキーを用いて入力コンテンツを暗号処理部６１３において暗号化し、これをメディア７００のユーザ領域に書き込む。この暗号化コンテンツは、通常の記録再生処理によって記録再生可能なユーザ領域に書き込まれる。
【０１７３】
このようにユーザデバイスにおいては、コンテンツに対応するＥＫＢを処理することにより得られるＥＫＢキーを用いて、コンテンツの暗号化に用いるコンテンツ毎に異なるコンテンツキーを暗号化し、その暗号化されたコンテンツキーと、記録対象となるコンテンツのコンテンツＩＤ、そのコンテンツの利用法を示す権利データ（rights data）とから成るＤＲＭを生成して記録する。権利データは、前述したように例えば再生やコピーの仕方に関するルールが記述される。具体的には、再生回数（play N times）,コピー回数（copy N times）,世代間コピー許容世代数（copy N generation）などがある。
【０１７４】
さらに、これらの情報を持つＤＲＭデータは改竄されないように、ＩＣＶによって保護される。ＩＣＶ、ＤＲＭデータに対し、記録毎に異なるＩＣＶキーにＥＫＢキーを作用させて得られる鍵（ＩＣＶ生成検証キー）を用いて生成される値であり、図２で説明したような処理、さらに具体的には例えばISO/IEC9797に記述されるＤＥＳ－ＭＡＣアルゴリズムが適用される。ユーザデバイスは、このＩＣＶの計算に用いられたＩＣＶキーおよび生成したＩＣＶの値自体をメディア上の保護領域に安全に格納し、コンテンツの再生、コピー処理など、ＤＲＭデータを利用する際にはこのＩＣＶをチェックすることによって、ＤＲＭデータの改竄が行なわれていないことを確認することができる。
【０１７５】
［改竄チェック値（ＩＣＶ）の記録処理］
ユーザデバイスにおけるＩＣＶの生成、記録処理の詳細を図１５の処理フローに従って説明する。
【０１７６】
まず、乱数発生装置などのキー・ジェネレータ２，６２１によってＩＣＶキーを生成（Ｓ

２０１）する。次にデバイスの有するキーセット（リーフキー、ノードキー）によって、ＥＫＢ処理部（Process ＥＫＢ）６１４においてＥＫＢの復号処理を実行する。ＥＫＢキーの取得に成功した場合（Ｓ２０２でＹｅｓ）は、ステップ２０３に進む。自デバイスがリボークされている場合などには、ＥＫＢの復号によってＥＫＢキーを取得できない（Ｓ２０２でＮｏ）ことになり、処理は終了する。

【０１７７】

次に、キー・ジェネレータ６２１によって生成されたＩＣＶキーにＥＫＢキーを作用（ｅｘ．ＤＥＳ暗号化処理）させて鍵１（ＩＣＶ生成検証キー）を取得（Ｓ２０３）し、ＤＲＭデータ（権利データ、コンテンツＩＤ、暗号化コンテンツキー）に対して鍵１（ＩＣＶ生成検証キー）を作用させて図２の処理構成によって改竄チェック値（ＩＣＶ）を生成（Ｓ２０４）する。

【０１７８】

次に生成したＩＣＶキーとＩＣＶをメディアの保護領域に記録（Ｓ２０５）し、また、ＩＣＶのチェック対象データ、すなわちＤＲＭデータ（権利データ、コンテンツＩＤ、暗号化コンテンツキー）をメディアのユーザ領域に記録する。なお、ＩＣＶキーとＩＣＶは、メディアインタフェース６２４内の秘密情報記録再生専用回路としての専用ＩＣ６２５による処理、すなわち特定領域への書き込み処理、あるいは特定信号処理方式として実行される。

【０１７９】

［改竄チェック値（ＩＣＶ）によるデータ検証処理］

次に、上述のような方法によってメディアに書き込まれたＩＣＶを用いて検証対象のデータの改竄チェックを行なう処理について図１６の処理フローに従って説明する。

【０１８０】

まず、ＩＣＶ検証対象データ、この場合は、ＤＲＭデータ（権利データ、コンテンツＩＤ、暗号化コンテンツキー）をメディアのユーザ領域から読み出す（Ｓ３０１）。次に、メディアの保護領域からＩＣＶとＩＣＶキーの読み出し処理を実行する。前述したように保護領域に記録されたデータの再生は専用処理を実行する秘密情報記録再生専用回路としてのＩＣ（図１のＩＣ１９５）によって実行可能であり、専用ＩＣを持たないデバイスにおいては読み出しが不可能となる。

【０１８１】

メディアの保護領域からのＩＣＶとＩＣＶキーの読み出し処理に失敗した場合は、検証処理は実行できず、処理は終了する。専用処理を実行するＩＣを有するデバイスであり、ＩＣＶとＩＣＶキーの読み出し処理に成功した場合は、次ステップＳ３０３において、ＩＣＶ計算において利用されたＥＫＢをメディアのユーザ領域から読み出して、読み出したＥＫＢを自デバイスの格納キーセット（リーフキー、ノードキー）を用いて復号してＥＫＢキーを取得する。自デバイスがリボークされている場合などには、ＥＫＢの復号に失敗し、ＥＫＢキーを取得できないので、以後の処理が実行できず、処理を終了する。

【０１８２】

ＥＫＢを自デバイスの格納キーセット（リーフキー、ノードキー）を用いて復号してＥＫＢキーの取得に成功した場合は、ＩＣＶキーにＥＫＢを作用（ｅｘ．ＤＥＳ暗号処理）させて、鍵１（ＩＣＶ生成検証キー）を取得（Ｓ３０４）し、生成した鍵１（ＩＣＶ生成検証キー）により、ステップＳ３０１で読み出したＩＣＶ検証対象データ、すなわちＤＲＭデータ（権利データ、コンテンツＩＤ、暗号化コンテンツキー）をメッセージとして先の図２で説明した処理に従ってＩＣＶ’を生成（Ｓ３０５）する。

【０１８３】

ステップＳ３０６において、ＩＣＶ＝ＩＣＶ’が成立するか否かを判定し、成立しない場合は、検証対象データとしてのＤＲＭデータが改竄されていると判定し、処理を終了する。一方、ＩＣＶ＝ＩＣＶ’が成立する場合は検証対象データとしてのＤＲＭデータが改竄されていないと判定し、処理を終了する。

【０１８４】

［ユーザデバイスにおけるコンテンツ記録処理］
次に、ユーザデバイスにおけるコンテンツ記録処理について図１７の処理フローに従って説明する。
【０１８５】
まず、ユーザデバイスは、コンテンツを記録しようとするメディアからＥＫＢバージョンナンバを読み取る（Ｓ４０１）。要求ＥＫＢバージョン（Required EKB Version）は、メディアに対してコンテンツを記録する際に適用する最低のＥＫＢバージョンを示すナンバである。
【０１８６】
ＥＫＢは、前述したように、デバイスのリボークなどにおいて更新され、更新毎にバージョンナンバーが付与される。データ記録可能なメディアには、古いバージョンのＥＫＢを使用したコンテンツ記録を排除するため、最新のＥＫＢバージョンナンバーがユーザ領域に記録され、デバイスは適用しようとするＥＫＢのバージョンと、メディアに記録されたＥＫＢバージョンとの比較を実行して適用ＥＫＢバージョンがメディアに記録されたバージョンより古くない場合にのみＥＫＢを適用したコンテンツ記録を行なうことができる。
【０１８７】
ステップＳ４０２の比較処理において、適用ＥＫＢバージョンがメディアに記録されたバージョンより古いと判定されると、デバイスは、次ステップに移行せず処理を終了し、コンテンツの記録は実行されない。
【０１８８】
ステップＳ４０２の比較処理において、適用ＥＫＢバージョンがメディアに記録されたバージョンより古くないものと判定されると、次に、デバイスは、コンテンツキーを生成（Ｓ４０３）する。コンテンツキーは、キー・ジェネレータ１，６１１（図１４参照）で生成される。
【０１８９】
次にユーザデバイスは、ＤＲＭデータを生成（Ｓ４０４）する。ＤＲＭデータを構成する権利データと、コンテンツ識別子を取得し、さらに、暗号化コンテンツキーを加えてＤＲＭデータを生成する。暗号化コンテンツキーは、キー・ジェネレータ１，６１１で生成したコンテツキー（Ｋｃ）をＥＫＢキー（ｅｘ．ルートキー、キー暗号キー（ＫＥＫ））により、暗号処理部（Ｅｎｃ）６１２において暗号化して生成する。
【０１９０】
次に、乱数発生装置などのキー・ジェネレータ２，６２１によってＩＣＶキーを生成（Ｓ４０５）する。
【０１９１】
さらに、ステップＳ４０６において、デバイスの有するキーセット（リーフキー、ノードキー）によって、ＥＫＢ処理部（Process ＥＫＢ）６１４においてＥＫＢの復号処理を実行する。ＥＫＢキーの取得に成功した場合（Ｓ４０６でＹｅｓ）は、ステップ４０７に進む。自デバイスがリボークされている場合などには、ＥＫＢの復号によってＥＫＢキーを取得できない（Ｓ４０６でＮｏ）ことになり、処理は終了する。
【０１９２】
次に、キー・ジェネレータ６２１によって生成されたＩＣＶキーにＥＫＢキーを作用（ｅｘ．ＤＥＳ暗号化処理）させて鍵１（ＩＣＶ生成検証キー）を取得（Ｓ４０７）し、ＤＲＭデータ（権利データ、コンテンツＩＤ、暗号化コンテンツキー）に対して鍵１（ＩＣＶ生成検証キー）を作用させて図２の処理構成によって改竄チェック値（ＩＣＶ）を生成（Ｓ４０８）する。
【０１９３】
次に生成したＩＣＶキーとＩＣＶをメディアの保護領域に記録（Ｓ４０９）し、また、ＩＣＶのチェック対象データ、すなわちＤＲＭデータ（権利データ、コンテンツＩＤ、暗号化コンテンツキー）をメディアのユーザ領域に記録（Ｓ４１０）する。なお、ＩＣＶキーとＩＣＶは、メディアインタフェース６２４内の秘密情報記録再生専用回路としての専用

ＩＣ６２５による処理、すなわち特定領域への書き込み処理、あるいは特定信号処理方式として実行される。

【０１９４】

さらに、コンテンツをステップ４０３で生成したコンテンツキーを用いて暗号化してメディアのユーザ領域に記録（Ｓ４１１）して処理を終了する。

【０１９５】

［ユーザデバイスにおけるコンテンツ再生処理（ａ）］

次に、ユーザデバイスにおけるコンテンツ再生処理について説明する。ユーザデバイスとしての再生装置では、デジタルデータとしてコンテンツを記録したメディア（ｅｘ．ＣＤ，ＤＶＤなど）からメディアインタフェースを通してコンテンツを再生することができる。コンテンツは、暗号化されて記録されているので、復号処理が必要であり、また、再生時には、前述の改竄チェック値（ＩＣＶ）の検証を実行することが必要となる。

【０１９６】

さらに、前述のＤＲＭデータ中の権利データとして例えば再生回数制限、コピー回数制限などの様々な利用制限が付加されている場合、コンテンツ利用によりこれらの利用制限の更新が必要となる場合がある。この場合には、権利データの更新を実行するとともに、権利データを含むＤＲＭデータに基づく改竄チェック値（ＩＣＶ）を更新してメディアに書き込む処理が必要となる。

【０１９７】

メディアからのコンテンツ再生処理について図１８、図１９を用いて説明する。図１８を参照しながら図１９の処理フローに従って説明する。なお、図１８には、デバイスの暗号処理手段８１０（図１における暗号処理手段１５０に相当する）について、処理シーケンスに従って処理部を機能的に分割して示してあるが、これらの様々な処理部が個別に存在することを示すものではなく、各処理は暗号処理手段８１０が実行するものであり、説明のために各機能をブロックとして分割して示しているにすぎないものである。

【０１９８】

まず、ユーザデバイスは、再生対象コンテンツに対応するＤＲＭデータをメディア９００のユーザ領域から読み出す（Ｓ５０１）。ＤＲＭデータには、権利データ、コンテンツＩＤ、暗号化コンテンツキーが含まれる。

【０１９９】

次に、デバイスは、メディア９００の保護領域からコンテンツに対応するＩＣＶキー、ＩＣＶを読み出す。この読み出し処理は保護領域のデータ再生処理専用のＩＣ８３１を使用して実行される。従ってＩＣ８３１を持つデバイスにおいてのみ読み出しが可能となる。ステップＳ５０２におけるＩＣＶキー、ＩＣＶの読み出しに失敗すると、以降の再生処理フローシーケンスが停止され、再生処理エラーとして処理は終了する。

【０２００】

ステップＳ５０２におけるＩＣＶキー、ＩＣＶの読み出しに成功すると、ＩＣＶ計算に利用されたバージョンのＥＫＢをメディア９００のユーザ領域から読み出して、自デバイスのキーセット（リーフキー、ノードキー）を用いてＥＫＢ処理部８１１（図１８参照）においてＥＫＢの復号を実行し、ＥＫＢキーの取得を行なう（Ｓ５０３）。この時点で、デバイスのリボークがなされている場合などには、デバイスに格納されたキーセットを用いたＥＫＢ処理に失敗することになり、ＥＫＢキーの取得ができない。この場合は以降の再生処理フローシーケンスが停止され、再生処理エラーとして処理は終了する。

【０２０１】

デバイスに格納されたキーセットを用いたＥＫＢ処理に成功し、ＥＫＢキーの取得に成功すると、ステップＳ５０２で取得したＩＣＶキーにステップＳ５０３で取得したＥＫＢキーを鍵生成部（Ｆｕｎｃ）８１２において作用（ｅｘ．ＤＥＳ暗号化処理）させて鍵１（ＩＣＶ生成検証キー）を生成（Ｓ５０４）する。

【０２０２】

次にデバイスは、ステップＳ５０１でメディアのユーザ領域から読み出したＤＲＭデータ

に対して、ステップＳ５０４で生成した鍵１（ＩＣＶ生成検証キー）を用いて、前述の図２の構成に従ってＩＣＶ生成手段（Calculate ICV）８１３において検証用改竄チェック値（ＩＣＶ’）を生成（Ｓ５０５）する。

【０２０３】

次に、生成した検証用改竄チェック値（ＩＣＶ’）と、ステップＳ５０２でメディアから読み出したＩＣＶとの比較（Ｓ５０６）を行なう。ＩＣＶ＝ＩＣＶ’が成立すれば、ＤＲＭデータの改竄がないと判定され、次ステップに進む。ＩＣＶ＝ＩＣＶ’が成立しない場合は、ＤＲＭデータの改竄があると判定され、以降の再生処理フローシーケンスが停止され、再生処理エラーとして処理は終了する。

【０２０４】

ＩＣＶ＝ＩＣＶ’が成立した場合は、ＤＲＭデータ内の権利データのチェック（Ｓ５０７）を行なう。具体的には、例えば再生利用回数が制限内であるか否かのチェックなどである。再生許可がある場合は、次ステップに進む。再生許可がない場合は、以降の再生処理フローシーケンスが停止され、再生処理エラーとして処理は終了する。

【０２０５】

再生許可がある場合は、ＤＲＭデータの更新処理が必要か否かを判定（Ｓ５０８）し、必要であればＤＲＭデータの更新を実行する。具体的には、例えばＤＲＭデータの権利データ内に再生可能回数：Ｎなどの設定があった場合、再生可能回数をＮ－１に書き換える処理を実行する。さらに、書き換えたＤＲＭデータに基づいて改竄チェック値（ＩＣＶ）を新たに生成してこれを更新ＩＣＶとしてメディアに書き込む処理を実行する。

【０２０６】

このＤＲＭデータを更新した場合のＩＣＶ生成について、図１８の処理ブロック図を用いて説明する。デバイスは、乱数発生装置などのキー・ジェネレータ８２１によってＩＣＶキーを生成し、キー生成部（Ｆｕｎｃ）８２２において、ＩＣＶキーにＥＫＢキーを作用（ｅｘ．ＤＥＳ暗号化処理）させてＩＣＶ生成検証キーを生成する。

【０２０７】

さらに、ＩＣＶ生成検証キーを用いて更新したＤＲＭデータに対して図２を用いて説明したＩＣＶ生成処理をＩＣＶ生成手段（Calculate ICV）８２３において実行し、更新したＤＲＭデータに基づく更新した改竄チェック値（ＩＣＶ）を生成する。なお、生成したＩＣＶキー、ＩＣＶ、ＤＲＭデータは、それぞれメディアに格納する。これらの処理は、ＤＲＭデータの更新が必要な場合にのみ実行される。

【０２０８】

図１９のフローに戻ってコンテンツ再生処理についての説明を続ける。ステップＳ５０８において、ＤＲＭデータの更新が必要な場合は、ステップＳ５０９において上述のＤＲＭデータ更新、ＩＣＶ更新を実行する。ＤＲＭデータの更新が必要でない場合は、ステップＳ５０９を省略し、ステップＳ５１０に進む。

【０２０９】

ステップＳ５１０においては、ＤＲＭデータから暗号化コンテンツキーを取り出し、暗号処理部８２４において、ステップＳ５０３で取得したＥＫＢキーを用いて暗号化コンテンツキーの復号処理を実行する。さらに、ステップＳ５１１において、暗号処理部８２５においてコンテンツキーを用いて暗号化コンテンツの復号処理を実行してコンテンツを取得して再生を実行する。

【０２１０】

［ユーザデバイスにおけるコンテンツ再生処理（ｂ）］

次に、ユーザデバイスにおけるコンテンツ再生処理において、ＩＣＶ生成検証キーを生成する際のＥＫＢキーと、コンテンツキーＫｃの暗号化キーとしてのＥＫＢキーとが別々のＥＫＢによって格納されている場合の処理ついて図１８、図２０を用いて説明する。図１８を参照しながら図２０の処理フローに従って説明する。

【０２１１】

まず、ユーザデバイスは、再生対象コンテンツに対応するＤＲＭデータをメディア９００

のユーザ領域から読み出す（Ｓ５５１）。ＤＲＭデータには、権利データ、コンテンツＩＤ、暗号化コンテンツキーが含まれる。

【０２１２】

次に、デバイスは、メディア９００の保護領域からコンテンツに対応するＩＣＶキー、ＩＣＶを読み出す。この読み出し処理は保護領域のデータ再生処理専用のＩＣ８３１を使用して実行される。従ってＩＣ８３１を持つデバイスにおいてのみ読み出しが可能となる。ステップＳ５５２におけるＩＣＶキー、ＩＣＶの読み出しに失敗すると、以降の再生処理フローシーケンスが停止され、再生処理エラーとして処理は終了する。

【０２１３】

ステップＳ５５２におけるＩＣＶキー、ＩＣＶの読み出しに成功すると、次に、デバイス８００は、メディア９００のユーザ領域からＩＣＶ生成検証キーを生成する際のＥＫＢキーを格納したＥＫＢｉｃｖを取得し、自デバイスのキーセット（リーフキー、ノードキー）を用いてＥＫＢ処理部８１１（図１８参照）においてＥＫＢｉｃｖの復号を実行し、ＥＫＢｉｃｖキーの取得を行なう（Ｓ５５３）。この時点で、デバイスのリボークがなされている場合などには、デバイスに格納されたキーセットを用いたＥＫＢｉｃｖ処理に失敗することになり、ＥＫＢｉｃｖキーの取得ができない。この場合は以降の再生処理フローシーケンスが停止され、再生処理エラーとして処理は終了する。

【０２１４】

デバイスに格納されたキーセットを用いたＥＫＢｉｃｖ処理に成功し、ＥＫＢｉｃｖキーの取得に成功すると、ステップＳ５５２で取得したＩＣＶキーにステップＳ５５３で取得したＥＫＢｉｃｖキーを鍵生成部（Ｆｕｎｃ）８１２において作用（ｅｘ．ＤＥＳ暗号化処理）させて鍵１（ＩＣＶ生成検証キー）を生成（Ｓ５５４）する。

【０２１５】

次にデバイスは、ステップＳ５５１でメディアのユーザ領域から読み出したＤＲＭデータに対して、ステップＳ５５４で生成した鍵１（ＩＣＶ生成検証キー）を用いて、前述の図２の構成に従ってＩＣＶ生成手段（Calculate ICV）８１３において検証用改竄チェック値（ＩＣＶ’）を生成（Ｓ５５５）する。

【０２１６】

次に、生成した検証用改竄チェック値（ＩＣＶ’）と、ステップＳ５５２でメディアから読み出したＩＣＶとの比較（Ｓ５５６）を行なう。ＩＣＶ＝ＩＣＶ’が成立すれば、ＤＲＭデータの改竄がないと判定され、次ステップに進む。ＩＣＶ＝ＩＣＶ’が成立しない場合は、ＤＲＭデータの改竄があると判定され、以降の再生処理フローシーケンスが停止され、再生処理エラーとして処理は終了する。

【０２１７】

ＩＣＶ＝ＩＣＶ’が成立した場合は、ＤＲＭデータ内の権利データのチェック（Ｓ５５７）を行なう。具体的には、例えば再生利用回数が制限内であるか否かのチェックなどである。再生許可がある場合は、次ステップに進む。再生許可がない場合は、以降の再生処理フローシーケンスが停止され、再生処理エラーとして処理は終了する。

【０２１８】

再生許可がある場合は、コンテンツに対応するＥＫＢをメディア９００のユーザ領域から読み出して、自デバイスのキーセット（リーフキー、ノードキー）を用いてＥＫＢ処理部８１１（図１８参照）においてＥＫＢの復号を実行し、コンテンツキーの暗号化キーとしてのＥＫＢキーの取得を行なう（Ｓ５５８）。デバイスのリボークがなされている場合などには、デバイスに格納されたキーセットを用いたＥＫＢ処理に失敗することになり、ＥＫＢキーの取得ができない。この場合は以降の再生処理フローシーケンスが停止され、再生処理エラーとして処理は終了する。

【０２１９】

次に、ステップＳ５５９においては、ＤＲＭデータから暗号化コンテンツキーを取り出し、暗号処理部８２４において、ステップＳ５５８で取得したＥＫＢキーを用いて暗号化コンテンツキーの復号処理を実行する。さらに、ステップＳ５６０において、暗号処理部８

２５においてコンテンツキーを用いて暗号化コンテンツの復号処理を実行してコンテンツを取得して再生を実行する。

【０２２０】

なお、上記フローでは、ＤＲＭデータの更新処理については省略したが、ＤＲＭデータの更新が必要な場合は、前述の図１９のフローで説明したと同様のＤＲＭデータの更新処理を実行する。

【０２２１】

［デバイス間におけるコンテンツコピー処理］

次に異なるデバイス間におけるコンテンツコピー処理、すなわち一方のデバイスから他方のデバイスにコンテンツをコピーする処理について説明する。

【０２２２】

（ＳＡＣ（Secure Authenticated Channel）の確立）

なお、デバイス間のコンテンツ移動に際しては、デバイス間において相互認証処理を実行し、双方の通信相手の確認を実行する。

【０２２３】

図２１に、共通鍵暗号方式を用いた相互認証方法（ISO/IEC 9798-2）を示す。図２１においては、共通鍵暗号方式としてＤＥＳを用いているが、共通鍵暗号方式であれば他の方式も可能である。図２１において、まず、Ｂが６４ビットの乱数Ｒｂを生成し、Ｒｂおよび自己のＩＤであるＩＤ（ｂ）をＡに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａを生成し、Ｒａ、Ｒｂ、ＩＤ（ｂ）の順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いてデータを暗号化し、Ｂに返送する。なお、鍵Ｋａｂは、ＡおよびＢに共通の秘密鍵としてそれぞれの記録素子内に格納する鍵である。ＤＥＳのＣＢＣモードを用いた鍵Ｋａｂによる暗号化処理は、例えばＤＥＳを用いた処理においては、初期値とＲａとを排他的論理和し、ＤＥＳ暗号化部において、鍵Ｋａｂを用いて暗号化し、暗号文Ｅ１を生成し、続けて暗号文Ｅ１とＲｂとを排他的論理和し、ＤＥＳ暗号化部において、鍵Ｋａｂを用いて暗号化し、暗号文Ｅ２を生成し、さらに、暗号文Ｅ２とＩＤ（ｂ）とを排他的論理和し、ＤＥＳ暗号化部において、鍵Ｋａｂを用いて暗号化して生成した暗号文Ｅ３とによって送信データ（Token-AB）を生成する。

【０２２４】

これを受信したＢは、受信データを、やはり共通の秘密鍵としてそれぞれの記録素子内に格納する鍵Ｋａｂ（認証キー）で復号化する。受信データの復号化方法は、まず、暗号文Ｅ１を認証キーＫａｂで復号化し、乱数Ｒａを得る。次に、暗号文Ｅ２を認証キーＫａｂで復号化し、その結果とＥ１を排他的論理和し、Ｒｂを得る。最後に、暗号文Ｅ３を認証キーＫａｂで復号化し、その結果とＥ２を排他的論理和し、ＩＤ(ｂ)を得る。こうして得られたＲａ、Ｒｂ、ＩＤ(ｂ)のうち、ＲｂおよびＩＤ(ｂ)が、Ｂが送信したものと一致するか検証する。この検証に通った場合、ＢはＡを正当なものとして認証する。

【０２２５】

次にＢは、認証後に使用するセッションキー（Ｋｓｅｓ）を生成する（生成方法は、乱数を用いる）。そして、Ｒｂ、Ｒａ、Ｋｓｅｓの順に、ＤＥＳのＣＢＣモードで認証キーＫａｂを用いて暗号化し、Ａに返送する。

【０２２６】

これを受信したＡは、受信データを認証キーＫａｂで復号化する。受信データの復号化方法は、Ｂの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたＲｂ、Ｒａ、Ｋｓｅｓの内、ＲｂおよびＲａが、Ａが送信したものと一致するか検証する。この検証に通った場合、ＡはＢを正当なものとして認証する。互いに相手を認証した後には、セッションキーＫｓｅｓは、認証後の秘密通信のための共通鍵として利用される。

【０２２７】

なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【０２２８】

上述の認証処理においては、Ａ，Ｂは共通の認証キーＫａｂを共有する。この共通鍵Ｋａｂを上述の有効化キーブロック（ＥＫＢ）を使用してデバイスに配信する。

【０２２９】

例えば、図２１の例では、Ａ，またはＢのいずれかが双方において復号可能な有効化キーブロック（ＥＫＢ）によって認証キーＫａｂを暗号化して、他方に送信する構成としてもよいし、あるいは第３者がデバイスＡ，Ｂに対して双方が利用可能な有効化キーブロック（ＥＫＢ）を生成してデバイスＡ，Ｂに対して生成した有効化キーブロック（ＥＫＢ）によって認証キーＫａｂを暗号化して配信する構成としてもよい。

【０２３０】

図２２および図２３に複数のデバイスに共通の認証キーＫａｋｅを有効化キーブロック（ＥＫＢ）によって配信する構成例を示す。図２２はデバイス０，１，２，３に対して復号可能な認証キーＫａｋｅを配信する例、図２３はデバイス０，１，２，３中のデバイス３をリボーク（排除）してデバイス０，１，２に対してのみ復号可能な認証キーを配信する例を示す。

【０２３１】

図２２の例では、更新ノードキーＫ（ｔ）００によって、認証キーＫａｋｅを暗号化したデータ（ｂ）とともに、デバイス０，１，２，３においてそれぞれの有するノードキー、リーフキーを用いて更新されたノードキーＫ（ｔ）００を復号可能な有効化キーブロック（ＥＫＢ）を生成して配信する。それぞれのデバイスは、図２２の右側に示すようにまず、ＥＫＢを処理（復号）することにより、更新されたノードキーＫ（ｔ）００を取得し、次に、取得したノードキーＫ（ｔ）００を用いて暗号化された認証キー：Ｅｎｃ（Ｋ（ｔ）００，Ｋａｋｅ）を復号して認証キーＫａｋｅを得ることが可能となる。

【０２３２】

その他のデバイス４，５，６，７…は同一の有効化キーブロック（ＥＫＢ）を受信しても自身の保有するノードキー、リーフキーでは、ＥＫＢを処理して更新されたノードキーＫ（ｔ）００を取得することができないので、安全に正当なデバイスに対してのみ認証キーを送付することができる。

【０２３３】

一方、図２３の例は、図４の点線枠で囲んだグループにおいてデバイス３が、例えば鍵の漏洩によりリボーク（排除）されているとして、他のグループのメンバ、すなわち、デバイス０，１，２，に対してのみ復号可能な有効化キーブロック（ＥＫＢ）を生成して配信した例である。図２３に示す（ａ）有効化キーブロック（ＥＫＢ）と、（ｂ）認証キー（Ｋａｋｅ）をノードキー（Ｋ（ｔ）００）で暗号化したデータを配信する。

【０２３４】

図２３の右側には、復号手順を示してある。デバイス０，１，２は、まず、受領した有効化キーブロックから自身の保有するリーフキーまたはノードキーを用いた復号処理により、更新ノードキー（Ｋ（ｔ）００）を取得する。次に、Ｋ（ｔ）００による復号により認証キーＫａｋｅを取得する。

【０２３５】

図４に示す他のグループのデバイス４，５，６…は、この同様のデータ（ＥＫＢ）を受信したとしても、自身の保有するリーフキー、ノードキーを用いて更新ノードキー（Ｋ（ｔ）００）を取得することができない。同様にリボークされたデバイス３においても、自身の保有するリーフキー、ノードキーでは、更新ノードキー（Ｋ（ｔ）００）を取得することができず、正当な権利を有するデバイスのみが認証キーを復号して利用することが可能となる。

【０２３６】

このように、ＥＫＢを利用した認証キーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能とした認証キーを配信することが可能となる。

【０２３７】

上述の相互認証処理の結果デバイス相互はセッションキーを共有し、セッションキーを用

いた通信データの暗号化、復号処理を実行してセキュアな通信が実行可能となる。このようにデバイス間では、セキュアな通信路（ＳＡＣ：Secure Authenticated Channel）を確立した後、コンテンツ移動（コピー）が実行される。

【０２３８】

コピー処理におけるコンテンツデータ送信側とコンテンツデータ受信側の各デバイスにおける処理について、以下説明する。

【０２３９】

（ａ－１．データ送信側デバイスにおける処理）

まず、データの送信側の処理について説明する。データ送信側デバイスとしての再生装置では、デジタルデータとしてコンテンツを記録したメディア（ｅｘ．ＣＤ，ＤＶＤなど）からメディアインタフェースを通してコンテンツを読み出す。再生時には、前述の改竄チェック値（ＩＣＶ）の検証を実行することが必要となる。

【０２４０】

さらに、前述のＤＲＭデータ中の権利データとしてのコピー回数制限などの様々な利用制限が付加されている場合、コンテンツコピーによりこれらの利用制限の更新が必要となる。この場合には、権利データの更新を実行するとともに、権利データを含むＤＲＭデータに基づく改竄チェック値（ＩＣＶ）を更新してメディアに書き込む処理が必要となる。

【０２４１】

コンテンツコピー処理におけるデータ送信側の処理ついて図２４、図２５を用いて説明する。図２４を参照しながら図２５の処理フローに従って説明する。なお、図２４には、デバイス１０００の暗号処理手段１０１０（図１における暗号処理手段１５０に相当する）について、処理シーケンスに従って処理部を機能的に分割して示してあるが、これらの様々な処理部が個別に存在することを示すものではなく、各処理は暗号処理手段１０１０が実行するものであり、説明のために各機能をブロックとして分割して示しているにすぎないものである。

【０２４２】

まず、ユーザデバイス１０００は、コピー対象コンテンツに対応するＤＲＭデータをメディア１１００のユーザ領域から読み出す（Ｓ６０１）。ＤＲＭデータには、権利データ、コンテンツＩＤ、暗号化コンテンツキーが含まれる。

【０２４３】

次に、デバイス１０００は、ＤＲＭデータ中の権利データを参照し、コピーが許容されたコンテンツであるかを判定する（Ｓ６０２）。コピーが許容されない場合、以降のコピー処理フローシーケンスが停止され、処理エラーとして処理は終了する。コピーが許容される場合は、ステップＳ６０３において、コピー対象コンテンツのＥＫＢを探索し、ステップＳ６０４において、自デバイスのキーセット（リーフキー、ノードキー）を用いてＥＫＢ処理部１１１１（図２４参照）においてＥＫＢの復号を実行し、ＥＫＢキーの取得を行なう。この時点で、デバイスのリボークがなされている場合などには、デバイスに格納されたキーセットを用いたＥＫＢ処理に失敗することになり、ＥＫＢキーの取得ができない。この場合は以降のコピー処理フローシーケンスが停止され、処理エラーとして処理は終了する。

【０２４４】

次に、デバイス１０００は、メディア１１００の保護領域からコンテンツに対応するＩＣＶキー、ＩＣＶを読み出す（Ｓ６０５）。この読み出し処理は保護領域のデータ再生処理専用の秘密情報記録再生専用回路としてのＩＣ１１３１を使用して実行される。従ってＩＣ１１３１を持つデバイスにおいてのみ読み出しが可能となる。

【０２４５】

ステップＳ６０５におけるＩＣＶキー、ＩＣＶの読み出しに成功すると、取得したＩＣＶキーにステップＳ６０４で取得したＥＫＢキーを鍵生成部（Ｆｕｎｃ）１１１２において作用（ｅｘ．ＤＥＳ暗号化処理）させて鍵１（ＩＣＶ生成検証キー）を生成（Ｓ６０６）する。

【０２４６】
次にデバイスは、ステップＳ６０１でメディアのユーザ領域から読み出したＤＲＭデータに対して、ステップＳ６０６で生成した鍵１（ＩＣＶ生成検証キー）を用いて、前述の図２の構成に従ってＩＣＶ生成手段（Calculate ICV）８１３において検証用改竄チェック値（ＩＣＶ’）を生成（Ｓ６０７）する。
【０２４７】
次に、生成した検証用改竄チェック値（ＩＣＶ’）と、ステップＳ６０５でメディアから読み出したＩＣＶとの比較（Ｓ６０８）を行なう。ＩＣＶ＝ＩＣＶ’が成立すれば、ＤＲＭデータの改竄がないと判定され、次ステップに進む。ＩＣＶ＝ＩＣＶ’が成立しない場合は、ＤＲＭデータの改竄があると判定され、以降のコピー処理フローシーケンスが停止され、処理エラーとして処理は終了する。
【０２４８】
ＩＣＶ＝ＩＣＶ’が成立した場合は、コピー先であるデバイスとの相互認証を実行し、ＳＡＣ（Secure Authenticated Channel）の確立に成功したか否かを判定する（Ｓ６０９）。なお、このＳＡＣ確立は、前述した相互認証（図２１参照）処理によって実行され、この際に用いる認証鍵Ｋａｂは、例えばコンテンツに対応するＥＫＢを復号することによって得られるデータに基づく鍵とすることができる。ＳＡＣ確立に失敗した場合は、コピー先のデバイスが不正である可能性があり、以降のコピー処理フローシーケンスが停止され、処理エラーとして処理は終了する。
【０２４９】
ＳＡＣ（Secure Authenticated Channel）の確立に成功した場合は、ＤＲＭデータの更新を実行する（Ｓ６１０）。具体的には、例えばＤＲＭデータの権利データ内にコピー可能回数：Ｎなどの設定があった場合、コピー可能回数をＮ－１に書き換える処理を実行する。さらに、書き換えたＤＲＭデータに基づいて改竄チェック値（ＩＣＶ）を新たに生成してこれを更新ＩＣＶとしてメディアに書き込む処理を実行する。
【０２５０】
このＤＲＭデータを更新した場合のＩＣＶ生成について、図２４の処理ブロック図を用いて説明する。デバイスは、乱数発生装置などのキー・ジェネレータ１１２１によってＩＣＶキーを生成し、キー生成部（Ｆｕｎｃ）１１２２において、ＩＣＶキーにＥＫＢキーを作用（ｅｘ．ＤＥＳ暗号化処理）させてＩＣＶ生成検証キーを生成する。
【０２５１】
さらに、ＩＣＶ生成検証キーを用いて更新したＤＲＭデータに対して図２を用いて説明したＩＣＶ生成処理をＩＣＶ生成手段（Calculate ICV）１１２３において実行し、更新したＤＲＭデータに基づく更新した改竄チェック値（ＩＣＶ）を生成する。
【０２５２】
図２５のフローに戻ってコンテンツコピー処理についての説明を続ける。ステップＳ６１０において、ＤＲＭデータ更新、更新データ書き込み処理が終了すると、ステップＳ６１１において更新ＩＣＶの書き込みを実行する。
【０２５３】
次に、デバイス１０００は、コンテンツコピー先であるデバイス１２００との間で確立したＳＡＣを通してデバイス１２００にコピーコマンドを出力し、さらにメディア１１００から読み出した暗号化コンテンツ、ＤＲＭデータをデバイス１２００に送信する。
【０２５４】
（ａ－２．データ受信側デバイスにおける処理）
次に、データの受信側の処理について図２６、図２７を用いて説明する。図２６を参照しながら図２７の処理フローに従って説明する。なお、図２６には、デバイス１２００の暗号処理手段１２１０（図１における暗号処理手段１５０に相当する）について、処理シーケンスに従って処理部を機能的に分割して示してあるが、これらの様々な処理部が個別に存在することを示すものではなく、各処理は暗号処理手段１２１０が実行するものであり、説明のために各機能をブロックとして分割して示しているにすぎないものである。

【０２５５】
図２７の処理フローに従って説明する。まず、ユーザデバイスは、コピー元であるデバイスとの相互認証を実行し、ＳＡＣ（Secure Authenticated Channel）の確立に成功したか否かを判定（Ｓ７０１）する。なお、このＳＡＣ確立は、前述した相互認証（図２１参照）処理によって実行され、この際に用いる認証鍵Ｋａｂは、例えばコンテンツに対応するＥＫＢを復号することによって得られるデータに基づく鍵とすることができる。ＳＡＣ確立に失敗した場合は、コピー元のデバイスが不正である可能性があり、以降のコピー処理フローシーケンスが停止され、処理エラーとして処理は終了する。
【０２５６】
次に、デバイスは、コンテンツコピー元であるデバイスとの間で確立したＳＡＣを通してコピーコマンドを受信し、さらに暗号化コンテンツ、ＤＲＭデータをコピー元デバイスから受信（Ｓ７０２）する。
【０２５７】
次にユーザデバイスは、ＩＣＶ記録処理（Ｓ７０３）、を実行する。ＩＣＶ記録処理は、デバイス１２００の有するキーセット（リーフキー、ノードキー）によって、ＥＫＢ処理部（Process ＥＫＢ）１２１４においてＥＫＢの復号処理を実行する。ＥＫＢキーの取得に成功すると、次に、鍵生成部（Ｆｕｎｃ）１２２２において、キー・ジェネレータ１２２１によって生成されたＩＣＶキーにＥＫＢキーを作用（ｅｘ．ＤＥＳ暗号化処理）させて鍵１（ＩＣＶ生成検証キー）を取得し、ＩＣＶ生成手段（Calculate ICV）１２２３において、ＤＲＭデータ（権利データ、コンテンツＩＤ、暗号化コンテンツキー）に対して鍵１（ＩＣＶ生成検証キー）を作用させて図２の処理構成によって改竄チェック値（ＩＣＶ）を生成する。
【０２５８】
生成したＩＣＶキーとＩＣＶをメディアの保護領域に記録し、また、ＩＣＶのチェック対象データ、すなわちＤＲＭデータ（権利データ、コンテンツＩＤ、暗号化コンテンツキー）をメディアのユーザ領域に記録する。なお、ＩＣＶキーとＩＣＶは、メディアインタフェース１２２４内の秘密情報記録再生専用回路としての専用ＩＣ１２２５による処理、すなわち特定領域への書き込み処理、あるいは特定信号処理方式として実行される。さらに、受信した暗号化コンテンツをメディア１３００のユーザ領域に記録（Ｓ７０４）する。
【０２５９】
本構成においては、ＤＲＭデータの更新、ＩＣＶチェックがデータ送信側で実行されるので、データ受信側での処理負担は軽減される。次にデータ受信側でＩＣＶチェック、ＩＣＶ更新を行なう場合のデータ送信側およびデータ受信側処理について説明する。
【０２６０】
（ｂ－１．データ送信側デバイスにおける処理）
データ受信側でＩＣＶチェック、ＩＣＶ更新を行なう場合のデータ送信側処理について図２８のフローに従って説明する。ステップＳ８０１において、コピー対象コンテンツのＥＫＢを探索する。ＥＫＢの取得ができない場合は以降のコピー処理フローシーケンスが停止され、処理エラーとして処理は終了する。
【０２６１】
次に、ステップＳ８０２において、コピー先であるデバイスとの相互認証を実行し、ＳＡＣ（Secure Authenticated Channel）の確立に成功したか否かを判定する。なお、このＳＡＣ確立は、前述した相互認証（図２１参照）処理によって実行され、この際に用いる認証鍵Ｋａｂは、例えばコンテンツに対応するＥＫＢを復号することによって得られるデータに基づく鍵とすることができる。ＳＡＣ確立に失敗した場合は、コピー先のデバイスが不正である可能性があり、以降のコピー処理フローシーケンスが停止され、処理エラーとして処理は終了する。
【０２６２】
次に、ステップＳ８０３において、デバイスは、メディアの保護領域からコンテンツに対応するＩＣＶキー、ＩＣＶの読み出しを実行する。この読み出し処理は保護領域のデータ

再生処理専用のＩＣを使用して実行される。従ってＩＣを持つデバイスにおいてのみ読み出しが可能となる。読み出し不能の場合は、以降のコピー処理フローシーケンスが停止され、処理エラーとして処理は終了する。

【０２６３】

以上の処理が成功すると、デバイスは、コンテンツコピー先であるデバイスとの間で確立したＳＡＣを通してコピー先デバイスにコピーコマンドを出力し、さらにメディアから読み出した暗号化コンテンツ、ＤＲＭデータをコピー先デバイスに送信する。

【０２６４】

（ｂ－２．データ受信側デバイスにおける処理）

データ受信側でＩＣＶチェック、ＩＣＶ更新を行なう場合のデータ受信側処理について説明する。データ受信側デバイスとしての記録装置では、データ送信元から受信したデジタルデータとしてのコンテンツをメディア（ｅｘ．ＣＤ，ＤＶＤなど）に記録する。この際、ＤＲＭデータ中の権利データとしてのコピー回数制限の更新ＤＲＭデータに基づく改竄チェック値（ＩＣＶ）を更新してメディアに書き込む処理を実行する。

【０２６５】

コンテンツコピー処理におけるデータ受信側の処理ついて図２６を参照しながら図２９の処理フローに従って説明する。

【０２６６】

まず、ユーザデバイス１２００は、コピー元であるデバイス１０００との相互認証を実行し、ＳＡＣ（Secure Authenticated Channel）の確立に成功したか否かを判定（Ｓ９０１）する。なお、このＳＡＣ確立は、前述した相互認証（図２１参照）処理によって実行され、この際に用いる認証鍵Ｋａｂは、例えばコンテンツに対応するＥＫＢを復号することによって得られるデータに基づく鍵とすることができる。ＳＡＣ確立に失敗した場合は、コピー元のデバイスが不正である可能性があり、以降のコピー処理フローシーケンスが停止され、処理エラーとして処理は終了する。

【０２６７】

次に、デバイス１２００は、コンテンツコピー元であるデバイスとの間で確立したＳＡＣを通して暗号化コンテンツ、ＤＲＭデータ、ＩＣＶ、ＩＣＶキーを受信（Ｓ９０２）する。

【０２６８】

次にユーザデバイス１２００は、自デバイスのキーセット（リーフキー、ノードキー）を用いてＥＫＢ処理部１２１４（図２６参照）においてＥＫＢの復号を実行し、ＥＫＢキーの取得（Ｓ９０３）を行なう。この時点で、デバイスのリボークがなされている場合などには、デバイスに格納されたキーセットを用いたＥＫＢ処理に失敗することになり、ＥＫＢキーの取得ができない。この場合は以降のコピー処理フローシーケンスが停止され、処理エラーとして処理は終了する。

【０２６９】

次に、デバイス１２００は、受信したＩＣＶキーにステップＳ９０３で取得したＥＫＢキーを鍵生成部（Ｆｕｎｃ）１２２２において作用（ｅｘ．ＤＥＳ暗号化処理）させて鍵１（ＩＣＶ生成検証キー）を生成（Ｓ９０４）する。

【０２７０】

次にデバイスは、ステップＳ９０２でコピー元デバイス１０００から受信したＤＲＭデータに対して、ステップＳ９０４で生成した鍵１（ＩＣＶ生成検証キー）を用いて、前述の図２の構成に従ってＩＣＶ生成手段（Calculate ICV）１２２３において検証用改竄チェック値（ＩＣＶ’）を生成（Ｓ９０５）する。

【０２７１】

次に、生成した検証用改竄チェック値（ＩＣＶ’）と、ステップＳ９０２でコピー元デバイス１０００から受信したＩＣＶとの比較（Ｓ９０６）を行なう。ＩＣＶ＝ＩＣＶ’が成立すれば、ＤＲＭデータの改竄がないと判定され、次ステップに進む。ＩＣＶ＝ＩＣＶ’が成立しない場合は、ＤＲＭデータの改竄があると判定され、以降のコピー処理フローシ

ーケンスが停止され、処理エラーとして処理は終了する。

【０２７２】

ＩＣＶ＝ＩＣＶ’が成立した場合は、ＤＲＭデータの書き換え処理（Ｓ９０７）、ＩＣＶ記録処理（Ｓ９０８）、を実行する。ＩＣＶ記録処理は、デバイス１２００の有するキーセット（リーフキー、ノードキー）によって、ＥＫＢ処理部（Process ＥＫＢ）１２１４においてＥＫＢの復号処理を実行する。ＥＫＢキーの取得に成功すると、次に、鍵生成部（Ｆｕｎｃ）１２２２において、キー・ジェネレータ１２２１によって生成されたＩＣＶキーにＥＫＢキーを作用（ｅｘ．ＤＥＳ暗号化処理）させて鍵１（ＩＣＶ生成検証キー）を取得し、ＩＣＶ生成手段（Calculate ICV）１２２３において、ＤＲＭデータ（権利データ、コンテンツＩＤ、暗号化コンテンツキー）に対して鍵１（ＩＣＶ生成検証キー）を作用させて図２の処理構成によって改竄チェック値（ＩＣＶ）を生成する。

【０２７３】

生成したＩＣＶキーとＩＣＶをメディアの保護領域に記録し、また、ＩＣＶのチェック対象データ、すなわちＤＲＭデータ（権利データ、コンテンツＩＤ、暗号化コンテンツキー）をメディアのユーザ領域に記録する。なお、ＩＣＶキーとＩＣＶは、メディアインタフェース１２２４内の秘密情報記録再生専用回路としての専用ＩＣ１２２５による処理、すなわち特定領域への書き込み処理、あるいは特定信号処理方式として実行される。さらに、受信した暗号化コンテンツをメディア１３００のユーザ領域に記録（Ｓ９０９）する。

【０２７４】

本構成においては、ＩＣＶチェックをデータ受信側で実行するので、データ送信側での処理負担は軽減される。

【０２７５】

（ｃ－１．データ受信側デバイスにおける処理）

次に、コピー処理において、データ受信側で、コピー対象コンテンツを記録しようとするメディアにＥＫＢが格納されており、さらに、コピー対象コンテンツに付帯するＥＫＢが存在する場合に各ＥＫＢのバージョン比較を実行し、より新しいバージョンのＥＫＢをコンテンツに対応させて記録する処理を図３０の処理フローに従って説明する。

【０２７６】

まず、ユーザデバイスは、コピー元であるデバイスとの相互認証を実行し、ＳＡＣ（Secure Authenticated Channel）の確立に成功したか否かを判定（Ｓ１００１）する。なお、このＳＡＣ確立は、前述した相互認証（図２１参照）処理によって実行され、この際に用いる認証鍵Ｋａｂは、例えばコンテンツに対応するＥＫＢを復号することによって得られるデータに基づく鍵とすることができる。ＳＡＣ確立に失敗した場合は、コピー元のデバイスが不正である可能性があり、以降のコピー処理フローシーケンスが停止され、処理エラーとして処理は終了する。

【０２７７】

次に、デバイスは、コンテンツコピー元であるデバイスとの間で確立したＳＡＣを通してコピーコマンドを受信し、さらに暗号化コンテンツ、ＤＲＭデータをコピー元デバイスから受信（Ｓ１００２）する。

【０２７８】

次にユーザデバイスは、コピー対象コンテンツを記録しようとするメディアにＥＫＢが格納されているか否かを検証する。ＥＫＢが格納されていない場合は、ステップＳ１００７に進み、Ｓ１００７～Ｓ１００９の処理、ＤＲＭデータの書き換え処理、ＩＣＶ記録処理、暗号化コンテンツの記録処理を実行する。これらの処理は、図２７を参照して説明したコピー処理のＳ７０３～Ｓ７０５の処理と同様であり、説明を省略する。

【０２７９】

ステップＳ１００３において、コピー対象コンテンツを記録しようとするメディアにＥＫＢが格納されていると判定した場合は、ステップＳ１００４において、コンテンツに付随するＥＫＢと、メディア上のＥＫＢとのバージョン比較を実行する。ＥＫＢは、コンテンツコピー元のデバイスからコンテンツと共に送付されるＥＫＢである。

【０２８０】
コンテンツに付随するＥＫＢが新しい場合は、ステップＳ１００７に進み、Ｓ１００７～Ｓ１００９の処理、ＤＲＭデータの書き換え処理、ＩＣＶ記録処理、暗号化コンテンツの記録処理を実行する。これらの処理は、図２７を参照して説明したコピー処理のＳ７０３～Ｓ７０５の処理と同様であり、説明を省略する。
【０２８１】
メディアに格納されているＥＫＢがコンテンツに付随するＥＫＢより新しい場合は、ステップＳ１００５において、デバイスのキーセット（ノードキー、リーフキー）を用いてコンテンツに付随するＥＫＢからＥＫＢキー（ＥＫＢキー１）を取得し、さらに、メディアに格納されているＥＫＢからＥＫＢキー（ＥＫＢキー２）を取得する。
【０２８２】
次に、ＤＲＭデータ内の暗号化コンテンツキーの暗号化鍵の架け替え処理を実行する。すなわち、古いバージョンのＥＫＢキー、すなわちコンテンツに付随するＥＫＢのＥＫＢキー（ＥＫＢキー１）によって暗号化されていたコンテンツキーを復号し、新しいバージョンのＥＫＢキー、すなわちメディアに格納されているＥＫＢのＥＫＢキー（ＥＫＢキー２）によって再暗号化する処理を実行（Ｓ１００６）する。
【０２８３】
次に、ステップＳ１００７に進み、Ｓ１００７～Ｓ１００９の処理、すなわちＤＲＭデータの書き換え処理、ＩＣＶ記録処理、暗号化コンテンツの記録処理を実行する。なお、この際、コンテンツ付随のＥＫＢをメディアのＥＫＢに変更した場合は、コンテンツと対応するＥＫＢのメディア内の位置を示すポインタをメディアに記録する処理を実行する。
【０２８４】
この処理構成により、ＥＫＢの更新が促進される。すなわちコンテンツコピー時に、古いバージョンのＥＫＢが新しいバージョンのＥＫＢに書き換える処理が実行されることになり、例えばリボークされたデバイスでの古いバージョンのＥＫＢを使用した不正なコンテンツ利用の排除が促進されることになる。
【０２８５】
［メディアにおけるＥＫＢ、ＩＣＶの格納］
次にＣＤ，ＤＶＤ等、デジタルコンテンツを格納するメディアにおけるＥＫＢおよびＩＣＶ格納態様について説明する。
【０２８６】
これまでの説明から明らかなように、メディアにはコンテンツキーで暗号化された暗号化コンテンツが格納される。さらに、コンテンツキーを暗号化するＥＫＢキーを取得し、さらに、ＤＲＭデータの改竄チェック値（ＩＣＶ）の生成検証のためのＩＣＶ生成検証キーの生成のためのＥＫＢキーを格納したＥＫＢがユーザ領域に格納され、また、ＤＲＭデータに基づいて生成された改竄チェック値（ＩＣＶ）と、ＩＣＶ生成検証キーの生成に必要となるＩＣＶキーが保護領域に格納される。
【０２８７】
図３１に暗号化コンテンツ、ＥＫＢ、ＩＣＶ、ＩＣＶキーの格納態様の例を示す。図３１（Ａ）は、複数の暗号化コンテンツと、各コンテンツに対応するＥＫＢがそれぞれ対応付けられて各コンテンツの個別のＥＫＢがメディアのユーザ領域に格納された例である。コンテンツ１にはＥＫＢ１が対応付けられ、コンテンツ２にはＥＫＢ２が対応付けられ、コンテンツ３にはＥＫＢ３が対応付けられている。
【０２８８】
さらに、各々のコンテンツに対応するＤＲＭデータに基づいて生成された改竄チェック値（ＩＣＶｘ）と、ＩＣＶキーが個別に保護領域に格納される。
【０２８９】
なお、図３１（Ａ’）に示すように、メディアに格納した複数のコンテンツに１つのＥＫＢを対応させて、各コンテンツのコンテンツキーの暗号化キー、ＩＣＶ生成検証キーの生成のためのＥＫＢキーの取得に１つのＥＫＢを使用する構成とすることが可能であり、こ

の場合、各コンテンツにはそのヘッダ部分にＥＫＢの格納領域を示すポインタを設定するようにする。このような構成とすることで、データ容量が削減され、メディアの使用効率が高まる。

【０２９０】

メディア上における具体的な記録方式の例を、図３２（ａ）に示す。先に説明したような、ＥＦＭ変調を利用している場合には、メディア上には、ユーザ領域に記録されているコンテンツと同じ場所に、重畳するように保護領域が確保できる。従って、図３２（ａ）に示すようにコンテンツが記録されている領域と物理的に同じ場所に重ねて改竄チェック値（ＩＣＶｘ）と、ＩＣＶキーが記録され、前述した専用のＩＣを通してこれら改竄チェック値（ＩＣＶｘ）と、ＩＣＶキーの記録再生が実行される。記録されているコンテンツに対応するＩＣＶ及びＩＣＶキーを読み出すには、そのコンテンツが記録されている場所をスキャンすればよい。

【０２９１】

この図３２（ａ）に示す方法を用いる場合、ＤＲＭデータを更新し、ＩＣＶ及びＩＣＶキーを書き換えなければならない場合、メディアが再書き込み可能なものであるならば、そのまま記録されているＩＣＶ、ＩＣＶキーの値を書き換えればよい。

【０２９２】

しかし、再書き込み不可のメディアの場合には、記録されているユーザ領域のデータに影響を及ぼすことなく保護領域に記録されているデータのみを書き換えることが出来ないため、この方式を利用することは出来ない。この場合は、図３３（ｂ）に示すように、コンテンツ毎に、コンテンツが記録されている場所とは物理的に別の場所に、ＩＣＶおよびＩＣＶキーを格納し、これらをＤＲＭデータの更新に基づいて書き換えるようにする。

【０２９３】

また、予めＩＣＶ、ＩＣＶキーの更新データを格納する領域を確保し、確保領域に順次更新されたＩＣＶ、ＩＣＶキーを書き込むように構成してもよい。図３４（ｃ）（ｄ）は、コンテンツ１のＩＣＶポインタをコンテンツに連続した領域に書き込み、ＩＣＶポインタの示す位置を最初のＩＣＶ、ＩＣＶキーの格納領域として設定し、さらに、その後続部分に複数の更新ＤＲＭデータ用のＩＣＶとＩＣＶキーの格納領域を設けた構成である。（ｃ）は、一定バイト領域毎に更新ＩＣＶ、ＩＣＶキー格納領域を設定し、（ｄ）は、各領域にシーケンスナンバーを併せて格納し、シーケンスナンバーによって最新のデータを識別する構成としたものである。

【０２９４】

また、メディアに予め格納したＥＫＢ（メディアＥＫＢ）を持つ場合の例を図３５（ｂ）に示す。メディアＥＫＢは、例えばメディアの製造者が、コンテンツの書き込まれていないデータ書き込み可能なメディアを製造する場合に、その時点で最新のバージョンのＥＫＢをメディアに記録してユーザに提供する。このメディアＥＫＢを記録したメディアにコンテンツ書き込みを行なう場合、前述したように、ユーザは、メディアＥＫＢから取得したＥＫＢキーを利用してコンテンツキーの暗号化、さらに、ＩＣＶ生成検証キーの生成を実行する。このときのメディアのデータ格納構成は、図３５（Ｂ）に示すように、メディアＥＫＢがユーザ領域に格納され、メディアＥＫＢから取得したＥＫＢキーで暗号化されたコンテンツキーで暗号化したコンテンツがユーザ領域に１以上格納され、保護領域には、ＩＣＶとＩＣＶキーが格納されることになる。

【０２９５】

コンテンツキーを暗号化するＥＫＢキーと、ＩＣＶ生成検証キーを生成するためのＥＫＢキー（ＥＫＢｉｃｖ）を別々に持つ構成を図３５（Ｃ）に示す。この構成の場合、コンテンツキーを暗号化するＥＫＢキーを取得可能なＥＫＢは、図３１～３４で説明したと同様の様々な構成が可能であり、ＩＣＶ生成検証キーを生成するためのＥＫＢキー（ＥＫＢｉｃｖ）は、それらとは別にユーザ領域に格納される。

【０２９６】

このように、メディアに暗号化コンテンツを格納する場合、コンテンツキーを暗号化する

ＥＫＢキー取得用のＥＫＢ、ＤＲＭデータの改竄チェック値（ＩＣＶ）の生成検証のためのＩＣＶ生成検証キーの生成のためのＥＫＢキー取得用ＥＫＢがユーザ領域に格納され、また、ＤＲＭデータに基づいて生成された改竄チェック値（ＩＣＶ）と、ＩＣＶ生成検証キーの生成に必要となるＩＣＶキーが保護領域に格納される。

【０２９７】

なお、格納態様については、上述した例に限定されるものではなく、ＤＲＭデータに基づいて生成された改竄チェック値（ＩＣＶ）と、ＩＣＶ生成検証キーの記録再生が、ユーザ領域と異なり、専用ＩＣに基づいてのみ実行可能な構成とすればよい。

【０２９８】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０２９９】

【発明の効果】

以上、説明したように、本発明の情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム記憶媒体によれば、ＣＤ、ＤＶＤなどのデジタルデータ記録媒体（メディア）にコンテンツの利用制限情報からなる権利データ、暗号化コンテンツキーなどからなるＤＲＭデータを記録し、ＤＲＭデータに対する改竄チェック値（ＩＣＶ）を通常のデータ記録再生方式とは異なる専用ＩＣを介してのみ記録再生可能な領域（保護領域）に格納する構成としたので、権利データの書き換えによるコンテンツの不正利用が防止される。

【０３００】

さらに、本発明の構成によれば、ＩＣＶ生成検証用のキーを生成するためのキーをツリー（木）構造の鍵配布構成により配布するＥＫＢ配信により実行する構成としたので、ＥＫＢを復号可能な正当なデバイスにおいてのみＥＫＢキーの取得が実行可能となり、ＥＫＢキーの取得に基づくＩＣＶ検証、生成、さらにコンテンツ利用を実行可能としたので、不正デバイスの排除（リボーク）をＥＫＢの更新により、随時実行することが可能となる。

【０３０１】

さらに、本発明の構成によれば、ＩＣＶ生成検証用のキーを生成するためのキーをツリー（木）構造の鍵配布構成により配布するＥＫＢ配信により実行する構成とし、メディアに最新バージョンのメディアＥＫＢを格納してユーザに提供する構成とし、ユーザデバイスでは、ＥＫＢのバージョン比較を実行して、バージョンの新しいＥＫＢへの更新を実行する構成としたので、ＥＫＢの更新処理が促進され、不正デバイスによる古いバージョンのＥＫＢを使用したコンテンツ利用の早期排除が可能となる。

【図面の簡単な説明】

【図１】本発明のシステムにおいて適用可能な記録再生装置の構成例を示すブロック図である。

【図２】本発明のシステムにおいて適用可能な改竄チェック値（ＩＣＶ）生成、検証処理構成について説明する図である。

【図３】本発明のシステムにおいて適用可能な改竄チェック値（ＩＣＶ）生成、検証処理フローについて説明する図である。

【図４】本発明のシステムにおける各種キー、データの暗号化処理について説明するツリー構成図である。

【図５】本発明のシステムにおける各種キー、データの配布に使用される有効化キーブロック（ＥＫＢ）の例を示す図である。

【図６】本発明のシステムにおけるコンテンツキーの有効化キーブロック（ＥＫＢ）を使用した配布例と復号処理例を示す図である。

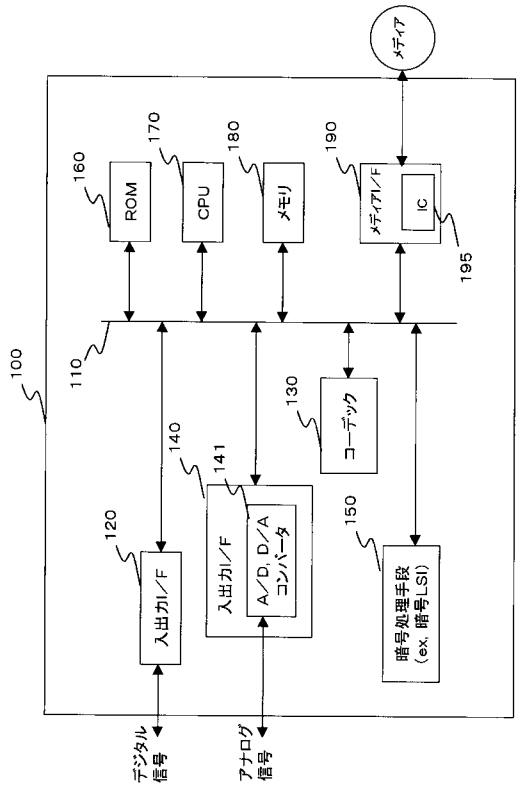
【図７】本発明のシステムにおける有効化キーブロック（ＥＫＢ）のフォーマット例を示

す図である。
【図８】本発明のシステムにおける有効化キーブロック（ＥＫＢ）のタグの構成を説明する図である。
【図９】本発明のシステムにおける有効化キーブロック（ＥＫＢ）と、コンテンツキー、コンテンツを併せて配信するデータ構成例を示す図である。
【図１０】本発明のシステムにおけるメディアのデータ格納構成例を示す図である。
【図１１】本発明のシステムにおけるコンテンツのメディアへの格納処理を実行するオーサリングデバイスの構成を示す図である。
【図１２】本発明のシステムにおけるコンテンツのメディアへの格納処理を実行するオーサリングデバイスの処理構成を示す図である。
【図１３】本発明のシステムにおけるコンテンツのメディアへの格納処理を実行するオーサリングデバイスの処理フローを示す図である。
【図１４】本発明のシステムにおけるコンテンツのメディアへの格納処理を実行するユーザデバイスの処理構成を示す図である。
【図１５】本発明のシステムにおけるＥＫＢキーを利用した改竄チェック値（ＩＣＶ）の生成、記録処理フローを示す図である。
【図１６】本発明のシステムにおけるＥＫＢキーを利用した改竄チェック値（ＩＣＶ）の検証処理フローを示す図である。
【図１７】本発明のシステムにおけるコンテンツのメディアへの格納処理を実行するユーザデバイスの処理フローを示す図である。
【図１８】本発明のシステムにおけるコンテンツのメディアからの再生処理を実行するユーザデバイスの処理構成を示す図である。
【図１９】本発明のシステムにおけるコンテンツのメディアからの再生処理を実行するユーザデバイスの処理フロー（例１）を示す図である。
【図２０】本発明のシステムにおけるコンテンツのメディアからの再生処理を実行するユーザデバイスの処理フロー（例２）を示す図である。
【図２１】本発明のシステムにおいて適用可能な共通鍵暗号方式による認証処理シーケンスを示す図である。
【図２２】本発明のシステムにおける有効化キーブロック（ＥＫＢ）と、認証キーを併せて配信するデータ構成と、デバイスでの処理例を示す図（その１）である。
【図２３】本発明のシステムにおける有効化キーブロック（ＥＫＢ）と、認証キーを併せて配信するデータ構成と、デバイスでの処理例を示す図（その２）である。
【図２４】本発明のシステムにおけるコンテンツのメディア間コピー処理を実行するコピー元ユーザデバイスの処理構成を示す図である。
【図２５】本発明のシステムにおけるコンテンツのメディア間コピー処理を実行するコピー元ユーザデバイスの処理フロー（例１）を示す図である。
【図２６】本発明のシステムにおけるコンテンツのメディア間コピー処理を実行するコピー先ユーザデバイスの処理構成を示す図である。
【図２７】本発明のシステムにおけるコンテンツのメディア間コピー処理を実行するコピー先ユーザデバイスの処理フロー（例１）を示す図である。
【図２８】本発明のシステムにおけるコンテンツのメディア間コピー処理を実行するコピー元ユーザデバイスの処理フロー（例２）を示す図である。
【図２９】本発明のシステムにおけるコンテンツのメディア間コピー処理を実行するコピー先ユーザデバイスの処理フロー（例２）を示す図である。
【図３０】本発明のシステムにおけるコンテンツのメディア間コピー処理を実行するコピー先ユーザデバイスの処理フロー（例３）を示す図である。
【図３１】本発明のシステムにおけるメディアにおけるデータ格納態様を示す図である。
【図３２】本発明のシステムにおけるメディアにおけるユーザ領域と保護領域のデータ格納態様（例１）を示す図である。
【図３３】本発明のシステムにおけるメディアにおけるユーザ領域と保護領域のデータ格

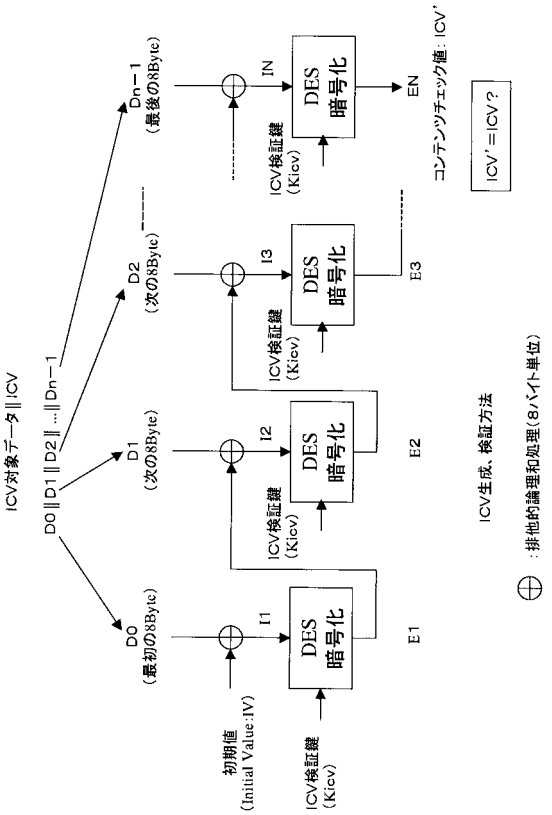
納態様（例２）を示す図である。
【図３４】本発明のシステムにおけるメディアにおけるユーザ領域と保護領域のデータ格納態様（例３）を示す図である。
【図３５】本発明のシステムにおけるメディアにおけるデータ格納態様を示す図である。
【符号の説明】
１００　記録再生装置
１１０　バス
１２０　入出力Ｉ／Ｆ
１３０　コーデック
１４０　入出力Ｉ／Ｆ
１４１　Ａ／Ｄ，Ｄ／Ａコンバータ
１５０　暗号処理手段
１６０　ＲＯＭ
１７０　ＣＰＵ
１８０　メモリ
１９０　メディアＩ／Ｆ
１９５　ＩＣ
２０１　バージョン
２０２　デプス
２０３　データポインタ
２０４　タグポインタ
２０５　署名ポインタ
２０６　データ部
２０７　タグ部
２０８　署名
３１０　保護領域
３１１　ＩＣＶキー
３１２　ＩＣＶ
３２０　ユーザ領域
３２１　ＥＫＢ
３２２　コンテンツキー
３２３　コンテンツ
３２４　ＥＫＢキー
３２５　コンテンツキー
３２６　ＤＲＭデータ
４００　オーサリングデバイス
４１０　バス
４２０　入出力Ｉ／Ｆ
４５０　暗号処理手段
４６０　ＲＯＭ
４７０　ＣＰＵ
４８０　メモリ
４９０　メディアＩ／Ｆ
４９５　ＩＣ
４１１　キー・ジェネレータ
４１２，４１３　暗号処理部
４２１　キー・ジェネレータ
４２２　キー生成手段
４２３　ＩＣＶ生成手段
４２４　メディアインタフェース

４２５　ＩＣ
５００　メディア
６００　デバイス
６１０　暗号処理手段
６１１　キー・ジェネレータ
６１２，６１３　暗号処理部
６１４　ＥＫＢ処理部
６２１　キー・ジェネレータ
６２２　キー生成手段
６２３　ＩＣＶ生成手段
６２４　メディアインタフェース
６２５　ＩＣ
７００　メディア
７１０　要求ＥＫＢバージョン
８００　デバイス
８１０　暗号処理手段
８１１　ＥＫＢ処理部
８１２　キー生成部
８１３　ＩＣＶ生成手段
８１４　ＩＣＶ比較処理手段
８１５　ＤＲＭデータ更新手段
８２１　キー・ジェネレータ
８２２　キー生成手段
８２３　ＩＣＶ生成手段
８２４，８２５　暗号処理部
８３０　メディアインタフェース
８３１　ＩＣ
９００　メディア
１０００　デバイス
１０１０　暗号処理手段
１１１１　ＥＫＢ処理部
１１１２　キー生成部
１１１３　ＩＣＶ生成手段
１１１４　ＩＣＶ比較処理手段
１１１５　ＤＲＭデータ更新手段
１１２１　キー・ジェネレータ
１１２２　キー生成手段
１１２３　ＩＣＶ生成手段
１１２４，１１２５　暗号処理部
１１３０　メディアインタフェース
１１３１　ＩＣ
１２００　デバイス
１２１０　暗号処理手段
１２１４　ＥＫＢ処理部
１２２１　キー・ジェネレータ
１２２２　キー生成手段
１２２３　ＩＣＶ生成手段
１２２４　メディアインタフェース
１２２５　ＩＣ
１３００　メディア

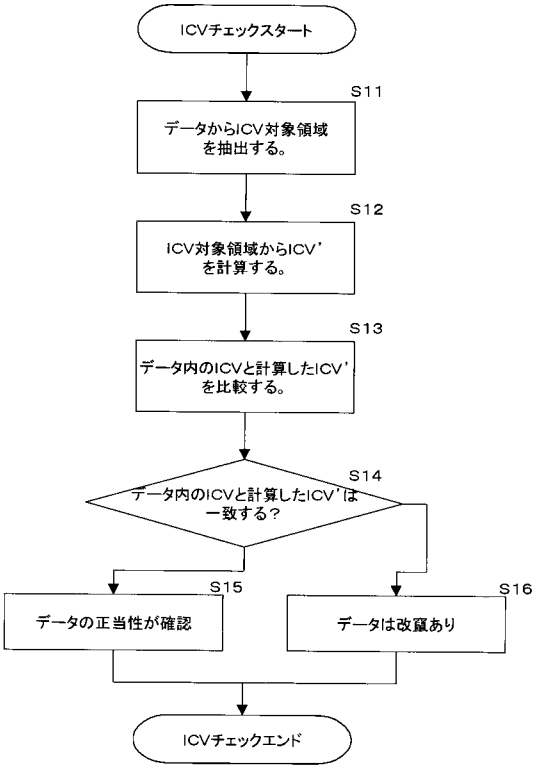
【図１】


メディア
ROM
CPU
メモリ
メディアI/F
IC
入出力I/F
入出力I/F
A/D, D/A コンバータ
コーデック
暗号処理手段 (ex. 暗号LSI)
デジタル信号
アナログ信号

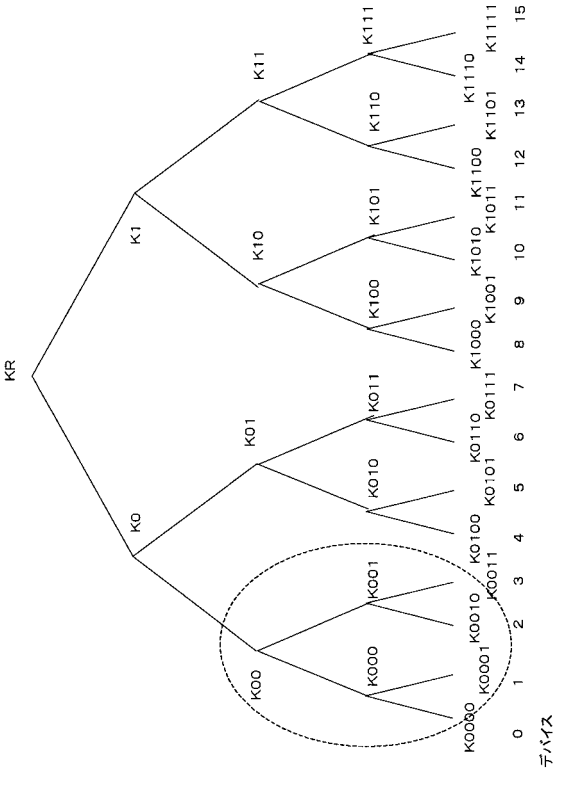
【図２】


ICV対象データ‖ICV
D0‖D1‖D2‖…‖Dn−1
D0 (最初の8Byte)
D1 (次の8Byte)
D2 (次の8Byte)
Dn−1 (最後の8Byte)
DES 暗号化
ICV検証鍵 (Kicv)
初期値 (Initial Value:IV)
コンテンツチェック値: ICV'
ICV'=ICV'?
ICV生成、検証方法
:排他的論理和処理(8バイト単位)

【図３】


ICVチェックスタート
S11
データからICV対象領域を抽出する。
S12
ICV対象領域からICV'を計算する。
S13
データ内のICVと計算したICV'を比較する。
S14
データ内のICVと計算したICV'は一致する?
S15
データの正当性が確認
S16
データは改竄あり
ICVチェックエンド

【図４】


KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
デバイス

【図５】

(A) 有効化キーブロック(EKB:Enabling Key Block) 例1

デバイス0, 1, 2にバージョン:tのノードキーを送付

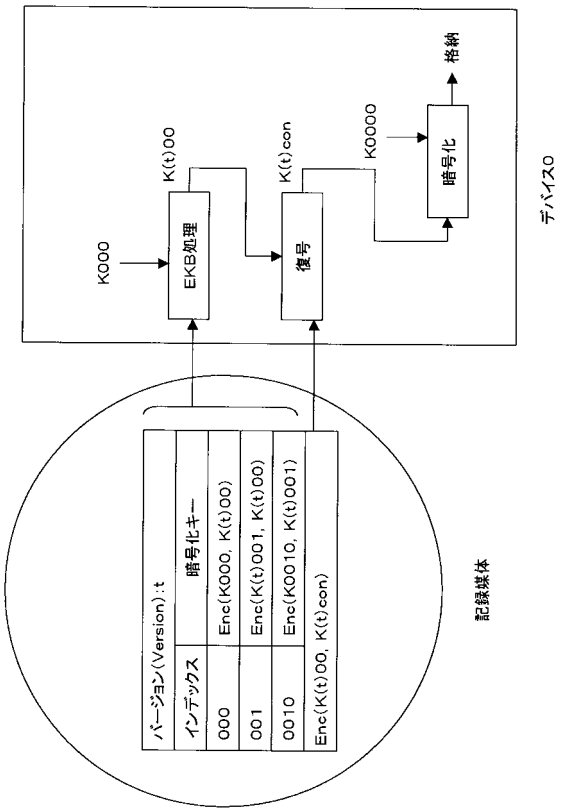
バージョン(Version):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

(B) 有効化キーブロック(EKB:Enabling Key Block) 例2

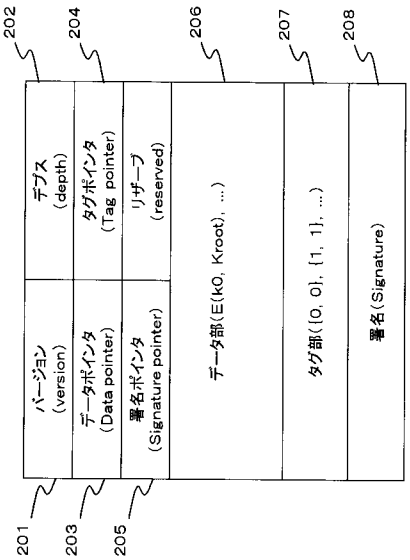
デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

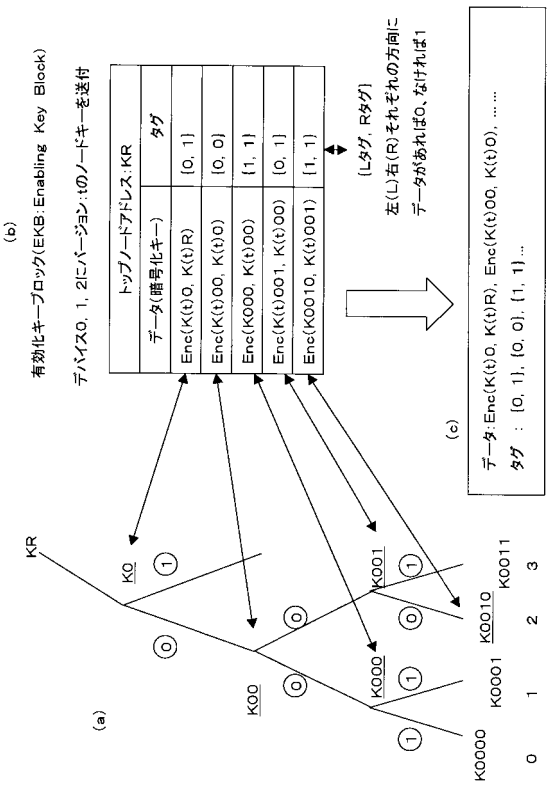
【図６】



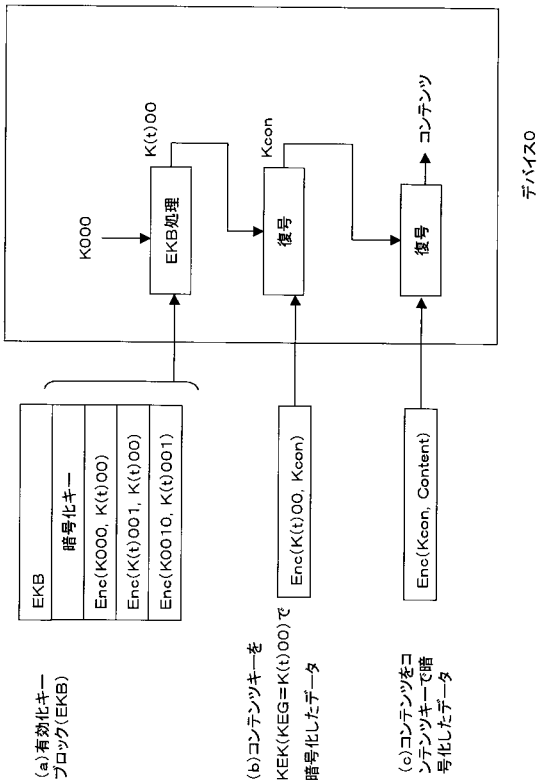
【図７】



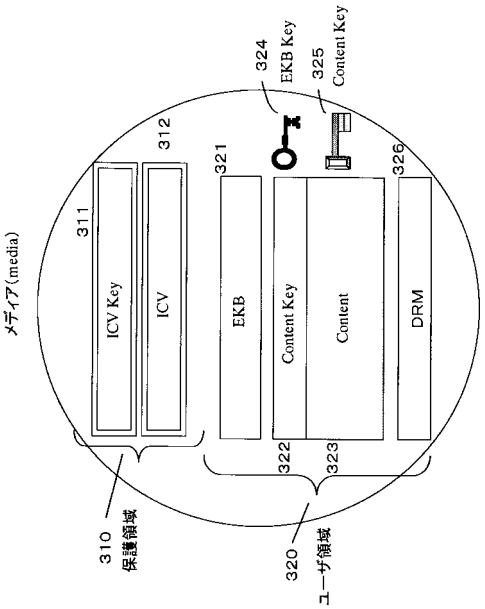
【図８】



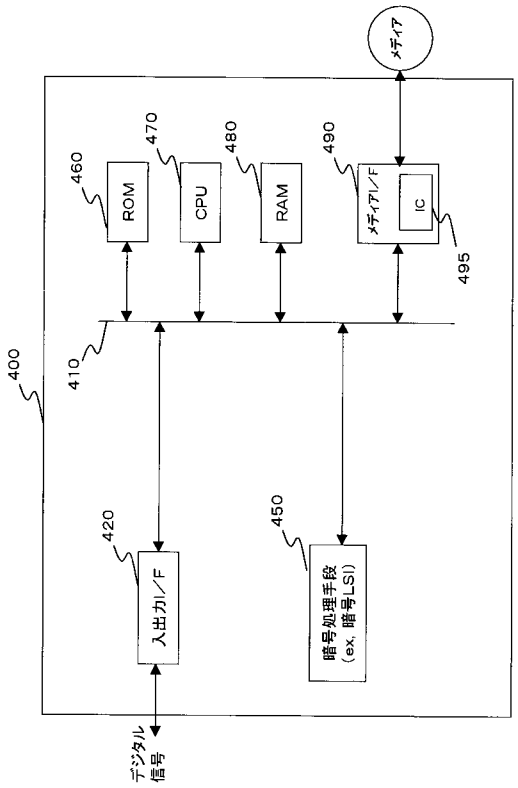
【図９】



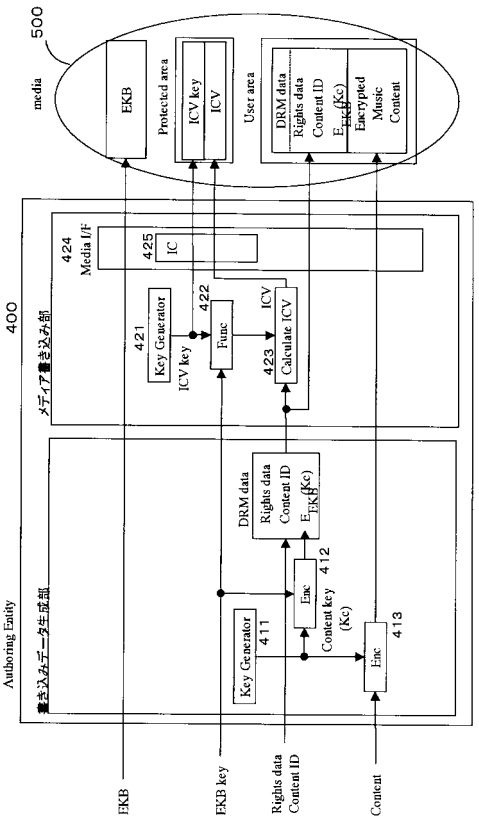
【図１０】



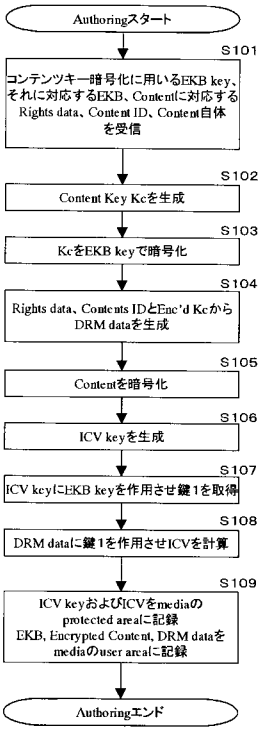
【図１１】



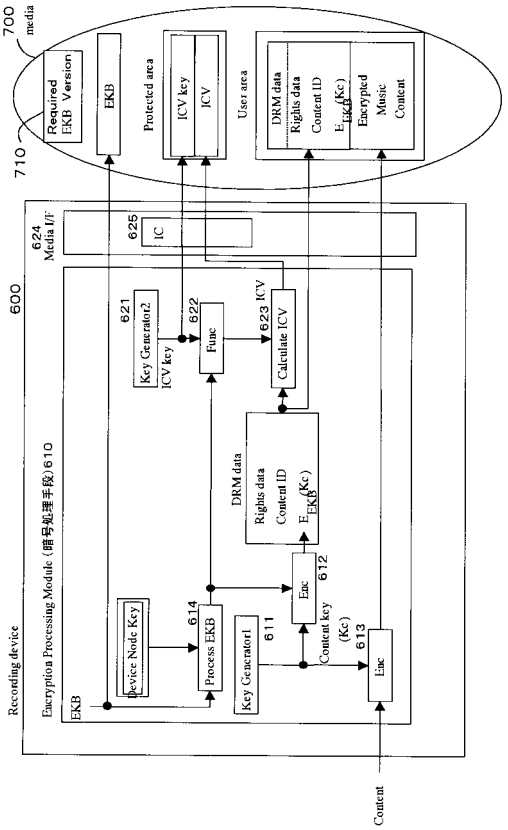
【図１２】



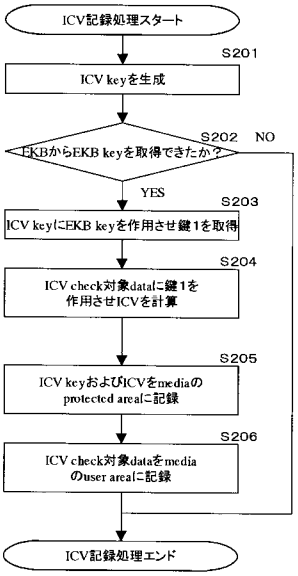
【図１３】



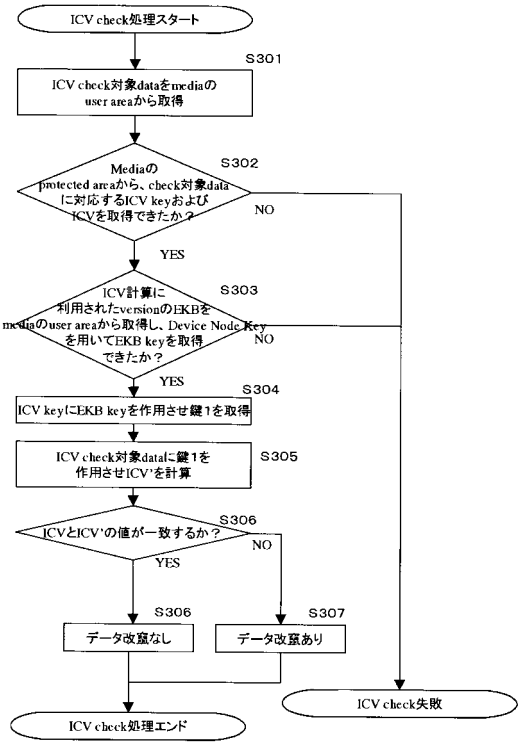
【図１４】



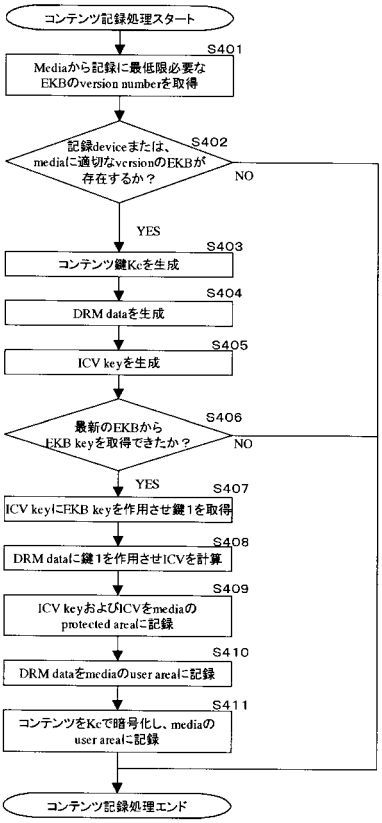
【図１５】



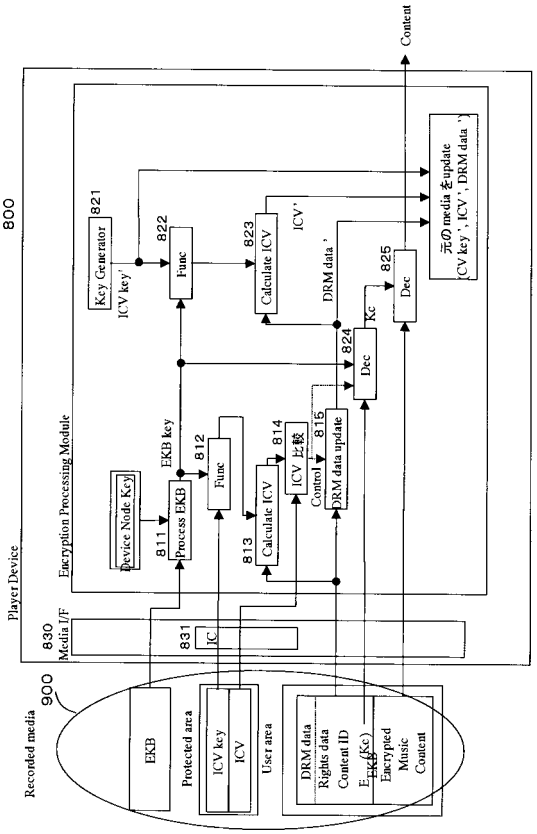
【図１６】



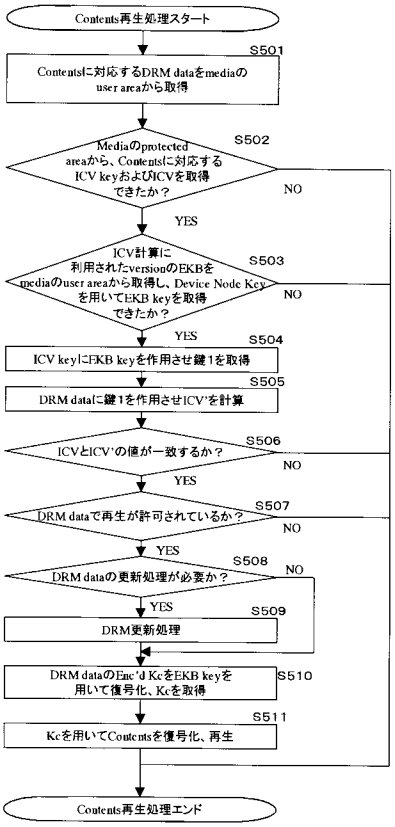
【図１７】



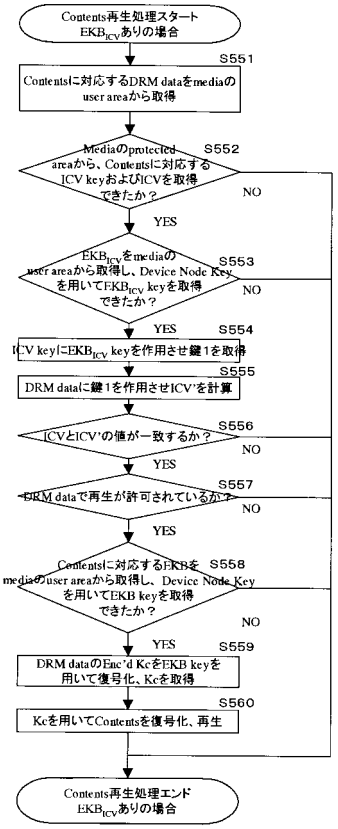
【図１８】



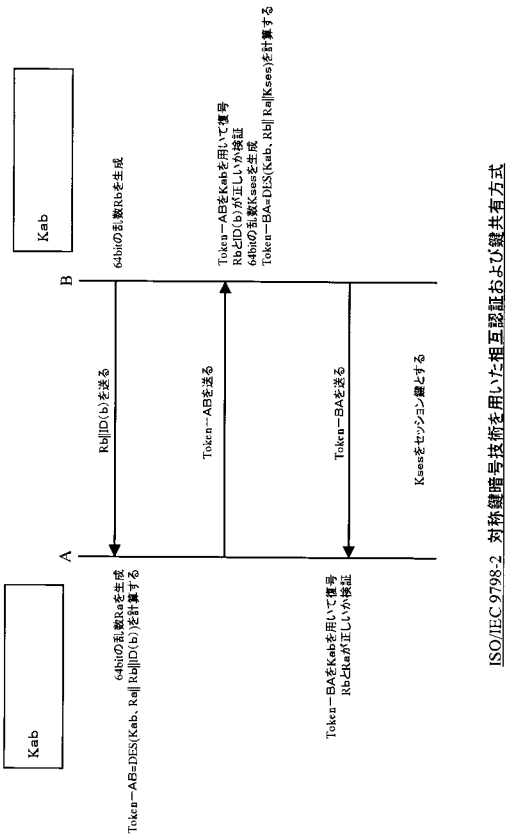
【図１９】



【図２０】

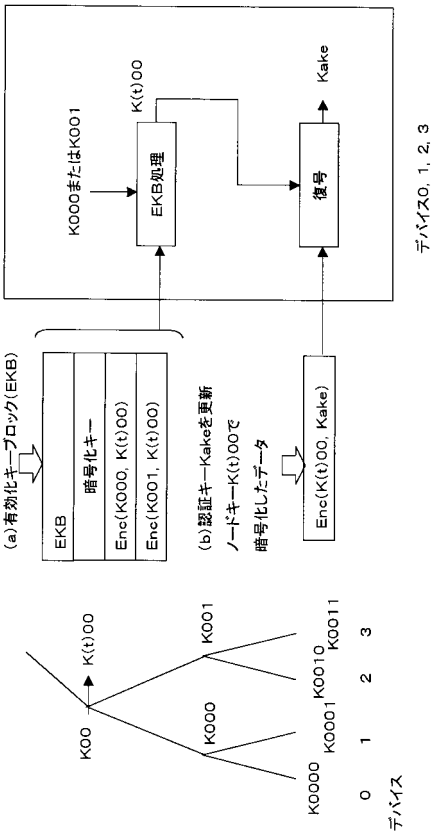


【図２１】

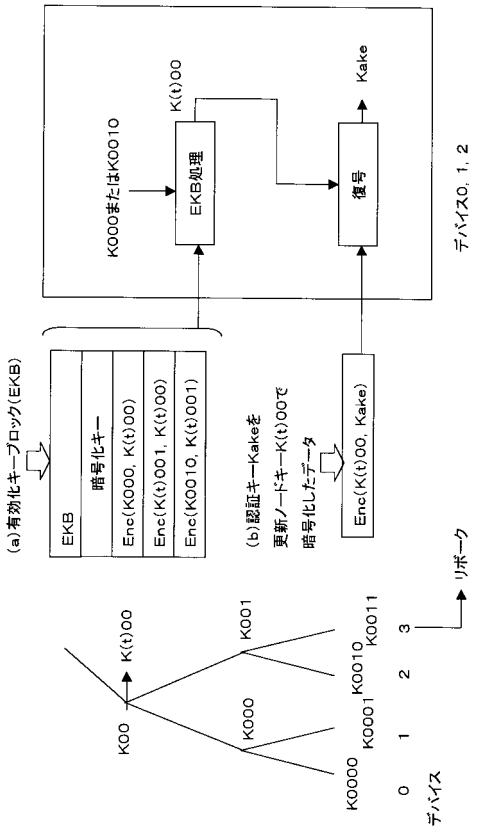


ISO/IEC 9798-2 対称鍵暗号技術を用いた相互認証および鍵共有方式

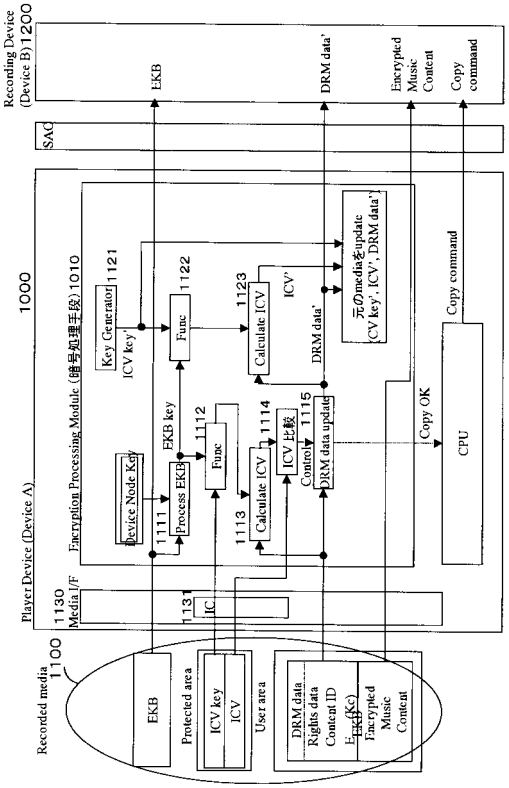
【図２２】



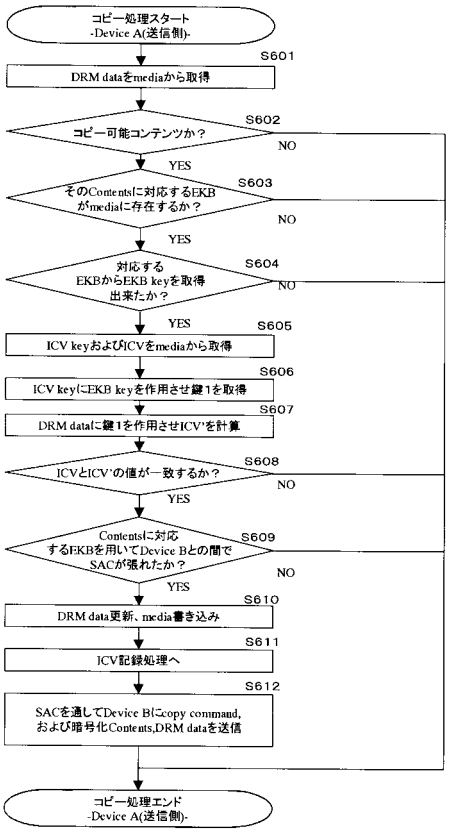
【図２３】



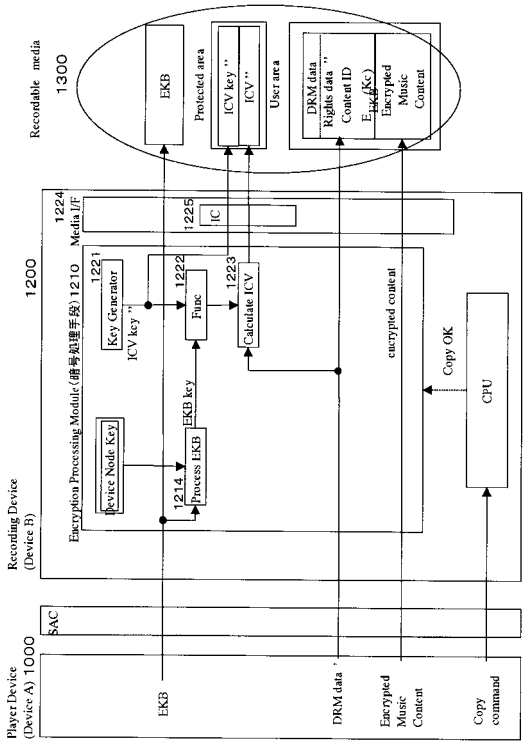
【図２４】



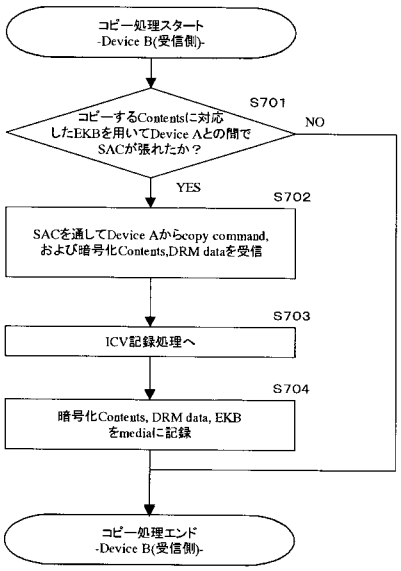
【図２５】



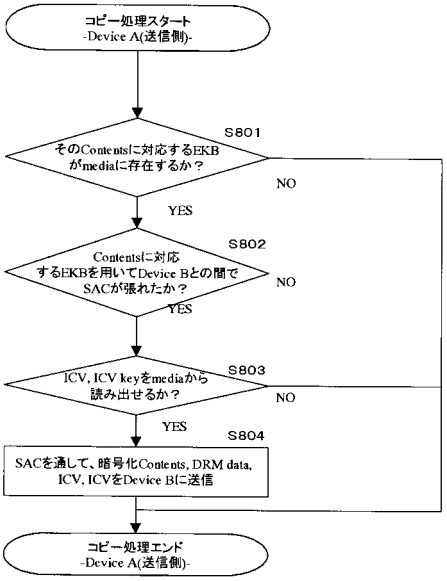
【図２６】



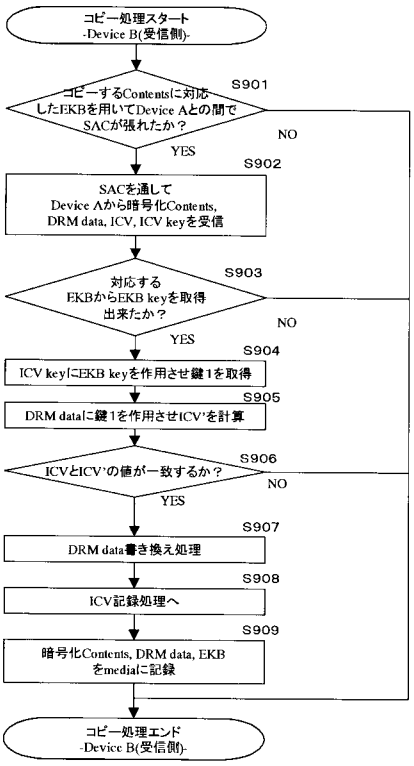
【図２７】



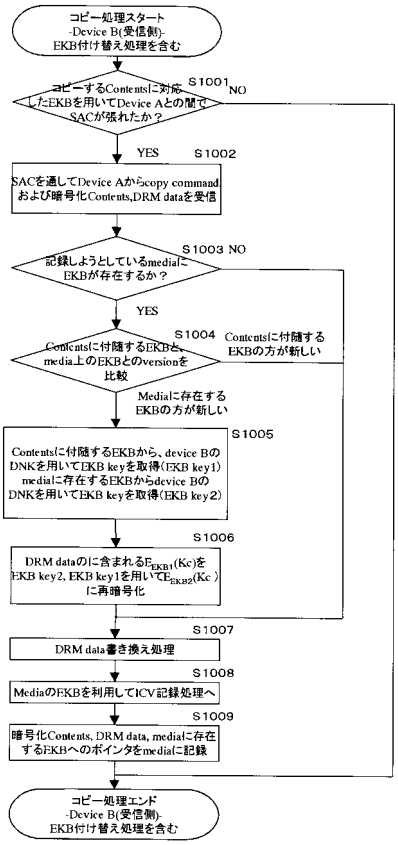
【図２８】



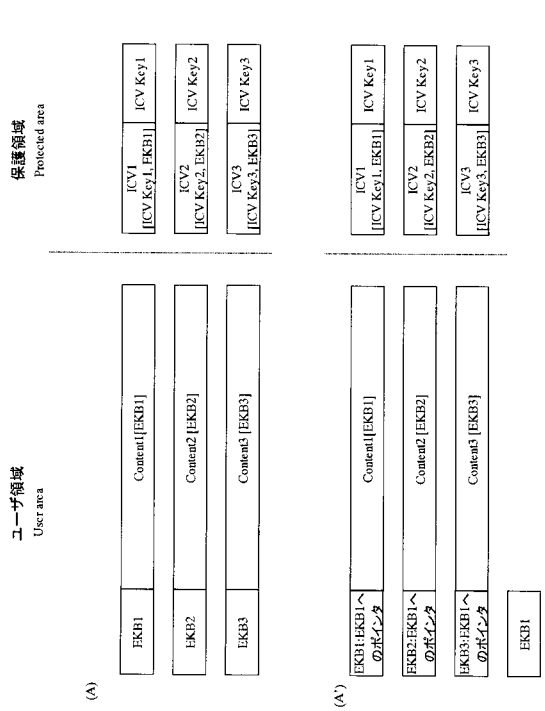
【図２９】



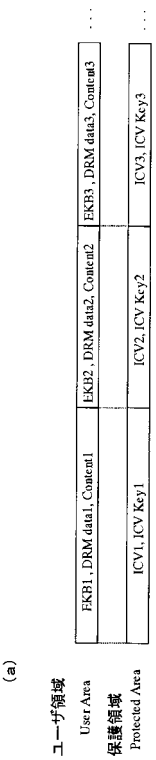
【図３０】



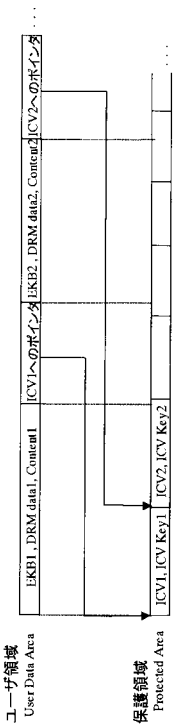
【図３１】



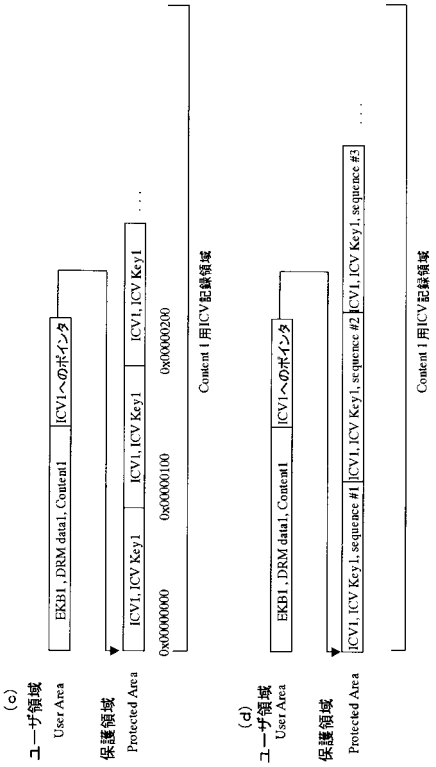
【図３２】



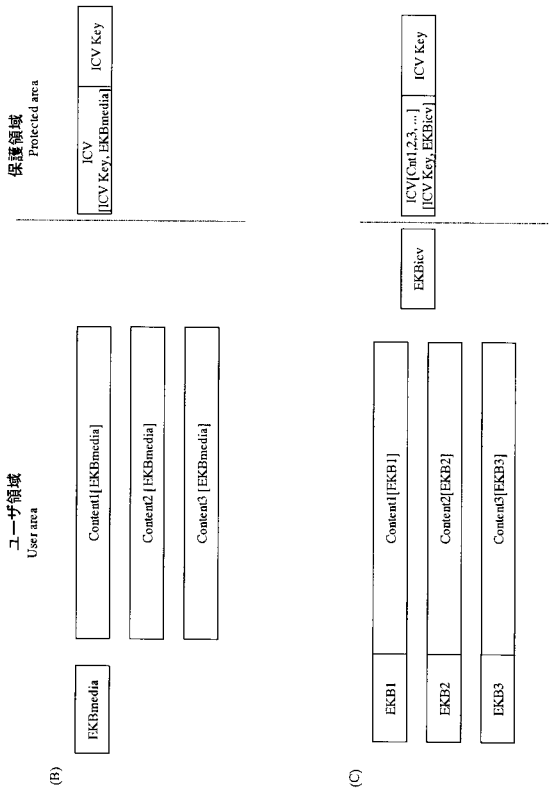
【図３３】


(b)
ユーザ領域
User Data Area
保護領域
Protected Area
EKB1, DRM data1, Content1
ICV1へのポインタ
EKB2, DRM data2, Content2
ICV2へのポインタ
ICV1, ICV Key1
ICV2, ICV Key2

【図３４】


(c)
ユーザ領域
User Area
保護領域
Protected Area
EKB1, DRM data1, Content1
ICV1へのポインタ
ICV1, ICV Key1
ICV1, ICV Key1
ICV1, ICV Key1
0x00000000
0x00000100
0x00000200
Content 1 用ICV記録領域
(d)
ユーザ領域
User Area
保護領域
Protected Area
EKB1, DRM data1, Content1
ICV1へのポインタ
ICV1, ICV Key1, sequence #1
ICV1, ICV Key1, sequence #2
ICV1, ICV Key1, sequence #3
Content 1 用ICV記録領域

【図３５】


(B)
ユーザ領域
User area
EKBmedia
Content1[EKBmedia]
Content2 [EKBmedia]
Content3 [EKBmedia]
保護領域
Protected area
ICV
[ICV Key, EKBmedia]
ICV Key
(C)
EKB1
EKB2
EKB3
Content1[EKB1]
Content2[EKB2]
Content3[EKB3]
EKBicv
ICV(Cnt1,2,3, ...)
[ICV Key, EKBicv]
ICV Key

フロントページの続き

(51)Int.Cl. F I
H04L 9/00 601A
H04L 9/00 601E

(72)発明者 大石 丈於
東京都品川区北品川６丁目７番３５号 ソニー株式会社内
(72)発明者 大澤 義知
東京都品川区北品川６丁目７番３５号 ソニー株式会社内

審査官 高橋 克

(56)参考文献 特開２０００－３３０８７０（ＪＰ，Ａ）
特開２０００－２４２９２９（ＪＰ，Ａ）
特開平１１－１８７０１３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
G06F 21/24
G09C 1/00
G11B 20/10
G11B 20/12
H04L 9/08